

102

NETWORK WIRETAPPING CAPABILITIES

Y 4. EN 2/3:103-168

Network Wiretapping Capabilities, S...

HEARING
BEFORE THE
SUBCOMMITTEE ON
TELECOMMUNICATIONS AND FINANCE
OF THE
COMMITTEE ON
ENERGY AND COMMERCE
HOUSE OF REPRESENTATIVES
ONE HUNDRED THIRD CONGRESS
SECOND SESSION

SEPTEMBER 13, 1994

Serial No. 103-168

Printed for the use of the Committee on Energy and Commerce



U.S. GOVERNMENT PRINTING OFFICE

86-474CC

WASHINGTON : 1995

For sale by the U.S. Government Printing Office
Superintendent of Documents, Congressional Sales Office, Washington, DC 20402
ISBN 0-16-046829-9

103
NETWORK WIRETAPPING CAPABILITIES

Y 4. EN 2/3: 103-168

Network Wiretapping Capabilities, S...

HEARING
BEFORE THE
SUBCOMMITTEE ON
TELECOMMUNICATIONS AND FINANCE
OF THE
COMMITTEE ON
ENERGY AND COMMERCE
HOUSE OF REPRESENTATIVES
ONE HUNDRED THIRD CONGRESS
SECOND SESSION

SEPTEMBER 13, 1994

Serial No. 103-168

Printed for the use of the Committee on Energy and Commerce



U.S. GOVERNMENT PRINTING OFFICE
WASHINGTON : 1995

86-474CC

For sale by the U.S. Government Printing Office
Superintendent of Documents, Congressional Sales Office, Washington, DC 20402
ISBN 0-16-046829-9

COMMITTEE ON ENERGY AND COMMERCE

JOHN D. DINGELL, Michigan, *Chairman*

HENRY A. WAXMAN, California
PHILIP R. SHARP, Indiana
EDWARD J. MARKEY, Massachusetts
AL SWIFT, Washington
CARDISS COLLINS, Illinois
MIKE SYNAR, Oklahoma
W.J. "BILLY" TAUZIN, Louisiana
RON WYDEN, Oregon
RALPH M. HALL, Texas
BILL RICHARDSON, New Mexico
JIM SLATTERY, Kansas
JOHN BRYANT, Texas
RICK BOUCHER, Virginia
JIM COOPER, Tennessee
J. ROY ROWLAND, Georgia
THOMAS J. MANTON, New York
EDOLPHUS TOWNS, New York
GERRY E. STUDDS, Massachusetts
RICHARD H. LEHMAN, California
FRANK PALLONE, Jr., New Jersey
CRAIG A. WASHINGTON, Texas
LYNN SCHENK, California
SHERROD BROWN, Ohio
MIKE KREIDLER, Washington
MARJORIE MARGOLIES-MEZVINSKY,
Pennsylvania
BLANCHE M. LAMBERT, Arkansas

CARLOS J. MOORHEAD, California
THOMAS J. BLILEY, Jr., Virginia
JACK FIELDS, Texas
MICHAEL G. OXLEY, Ohio
MICHAEL BILIRAKIS, Florida
DAN SCHAEFER, Colorado
JOE BARTON, Texas
ALEX McMILLAN, North Carolina
J. DENNIS HASTERT, Illinois
FRED UPTON, Michigan
CLIFF STEARNS, Florida
BILL PAXON, New York
PAUL E. GILLMOR, Ohio
SCOTT KLUG, Wisconsin
GARY A. FRANKS, Connecticut
JAMES C. GREENWOOD, Pennsylvania
MICHAEL D. CRAPO, Idaho

ALAN J. ROTH, *Staff Director and Chief Counsel*

DENNIS B. FITZGIBBONS, *Deputy Staff Director*

MARGARET A. DURBIN, *Minority Chief Counsel and Staff Director*

SUBCOMMITTEE ON TELECOMMUNICATIONS AND FINANCE

EDWARD J. MARKEY, Massachusetts, *Chairman*

W.J. "BILLY" TAUZIN, Louisiana
RICK BOUCHER, Virginia
THOMAS J. MANTON, New York
RICHARD H. LEHMAN, California
LYNN SCHENK, California
MARJORIE MARGOLIES-MEZVINSKY,
Pennsylvania
MIKE SYNAR, Oklahoma
RON WYDEN, Oregon
RALPH M. HALL, Texas
BILL RICHARDSON, New Mexico
JIM SLATTERY, Kansas
JOHN BRYANT, Texas
JIM COOPER, Tennessee
JOHN D. DINGELL, Michigan
(*Ex Officio*)

JACK FIELDS, Texas
THOMAS J. BLILEY, Jr., Virginia
MICHAEL G. OXLEY, Ohio
DAN SCHAEFER, Colorado
JOE BARTON, Texas
ALEX McMILLAN, North Carolina
J. DENNIS HASTERT, Illinois
PAUL E. GILLMOR, Ohio
CARLOS J. MOORHEAD, California
(*Ex Officio*)

DAVID H. MOULTON, *Chief Counsel/Staff Director*

GERARD WALDRON, *Counsel*

COLIN CROWELL, *Telecommunications Policy Analyst*

CATHERINE REID, *Minority Counsel*

MICHAEL REGAN, *Minority Counsel*

CONTENTS

	Page
Testimony of:	
Bart, Daniel L., Vice President, Technical and Regulatory Affairs, Telecommunications Industry Association	148
Berman, Jerry, J. Policy Director, Electronic Frontier Foundation, Inc.	115
Freeh, Hon. Louis J., Director, Federal Bureau of Investigation	9
Metzger, A. Richard, Deputy Chief, Common Carrier Bureau, Federal Communications Commission	79
Neel, Roy, President and Chief Executive Officer, United States Telephone Association	101
Reilly, Thomas, District Attorney, Middlesex County, Cambridge, MA.	77
Wheeler, Thomas, President, Cellular Telecommunications Industry Association	139
Material submitted for the record by:	
Energy and Commerce Committee: Letter dated September 20, 1994 from Hon. John D. Dingell, to Hon. Thomas S. Foley, The Speaker, U.S. House of Representatives re H.R. 4922	168
International Association of Chiefs of Police: Letter dated September 7, 1994 to Hon. Edward J. Markey, from Sylvester Daughtry, President	171
Justice Department, Federal Bureau of Investigation: Letter dated April 15, 1993 to Hon. Edward J. Markey, from William S. Sessions, Director, with attached news release from The White House	172
National District Attorneys Association: Letter dated September 2, 1994 to Hon. Edward J. Markey, from Robert L. Deschamps, President, with attached resolution	182

NETWORK WIRETAPPING CAPABILITIES

TUESDAY, SEPTEMBER 13, 1994

HOUSE OF REPRESENTATIVES,
COMMITTEE ON ENERGY AND COMMERCE,
SUBCOMMITTEE ON TELECOMMUNICATIONS AND FINANCE,
Washington, DC.

The subcommittee met, pursuant to notice, at 10:30 a.m., in room 2123, Rayburn House Office Building, Hon. Edward J. Markey (chairman) presiding.

Mr. MARKEY. Good morning. The topic of today's hearing is an important one that must be addressed amidst all the talk of a communications revolution. How do we balance the growth of the communications industry and its advances in technology, something this subcommittee has taken pains to promote, with the legitimate needs of law enforcement for wiretap capabilities.

The Judiciary Committee is about to report H.R. 4922, the "Digital Telephony and Communications Privacy Act of 1994." Though the subcommittee does not yet have formal jurisdiction over that legislation, the short time left in this session of Congress requires that we address these issues in the bill today. This will ensure that we have adequate time to explore these issues and help fashion a workable solution that serves the legitimate needs of law enforcement while not unduly interfering with the telecommunications industry.

The issue of wiretapping telephone lines has dogged constitutional, privacy, and telecommunications advocates for decades. In fact, wiretap law reflects a 65-year history between Congress and the courts. In 1928, the Supreme Court first confronted the issue in *Olmstead v. United States*. In this famous case, the court held that tapping a telephone line does not constitute a "search or seizure" and, therefore, does not violate the fourth amendment.

This case is most famous, however, for a dissent by Justice Brandeis, who argued that the Constitution protected citizens against wiretaps. In that great Justice's most memorable phrase, he wrote that the fourth amendment protected against wiretaps because it protected the right of privacy, which he defined as "the right to be let alone—the most comprehensive of rights and the right most valued by civilized man."

Congress responded to the Court's decision in *Olmstead* and the force of Justice Brandeis' dissent just 6 years later in passing the Communications Act of 1934. Congress included a provision in section 705 that states, "No person not being authorized by the sender shall intercept any communication and divulge or publish [its] existence, contents—or meaning." However, courts quickly construed

section 705 to permit Federal and State law enforcement to use a wiretap for investigation purposes so long as they did not divulge any content by testifying about it in open court.

Then, in 1967, the Supreme Court finally adopted Justice Brandeis' dissenting view, overruled *Olmstead*, and held that an eavesdropping does amount to a "search or seizure" and thus was protected by the Constitution.

Just 1 year later, Congress again responded by passing the 1968 Wiretap Act. This law makes wiretaps lawful by setting up a judicial process that law enforcement must go through to get a court-ordered wiretap.

But the story does not end there. Congress again responded to changes in computer and in communications technology by passing the "Electronic Communications Privacy Act of 1986." This law, which was sponsored by Senator Leahy and Congressman Edwards, amended the 1968 Wiretap Act by protecting a new class of electronic communications, defined broadly to include everything from e-mail to databases. That legislation reflected an ongoing effort to update and clarify Federal wiretap laws, as the Senate committee put it, "in light of dramatic changes in new computer and telecommunications technologies."

Well, today we are back at the task of updating and clarifying our wiretap law again. This time, the changes in computer and telecommunications technology are not just dramatic; they are overwhelming. The growth of digital communications over the past 8 years, the spread of fiber deeper into the local phone network, the spread and growth of wireless services—all of these developments converge to set the stage for today's hearing.

The Federal Bureau of Investigation says that as these advanced technologies get deployed, that the technology should not, in essence, repeal or modify the 1968 Wiretap Act. Instead, the Bureau argues we must update and clarify our laws so that their ability to conduct wiretaps is maintained—not expanded and not diminished—just maintained.

Therefore, as I see it, the challenge before the subcommittee is to listen to the FBI and to local law enforcement, who are on the front lines battling crime; and then to listen to the telecommunications industry, which is in the forefront of trying to develop new telecommunications equipment and services. And then to try to reconcile these views, working with the Judiciary Committee, to come up with a policy that, one, protects the privacy interests of our citizens; two, is mindful of the limited financial resources of taxpayers or ratepayers; three, meets the legitimate needs of law enforcement; and four, does not unduly interfere with our telecommunications industry, which is racing to the future with advances in communications technology.

I think the bill introduced by Congressmen Edwards and Hyde represents great progress in meeting these criteria, and they and their staffs should be commended for the substantial effort it took to make that progress. But clearly more work needs to be done.

I look forward to the hearing, as I am sure all the rest of the members do, so that we can assist in clarifying and crafting a workable solution to this genuine problem.

That concludes the opening statement of the Chair. Now the Chair will recognize the ranking minority member, the gentleman from Texas, Mr. Fields.

Mr. FIELDS. Thank you, Mr. Chairman. I want to congratulate you for calling today's timely hearing. Today, we are considering the need to ensure that law enforcement agencies will be able to carry out the investigative activities that Congress has specifically authorized through electronic surveillance in the 1986 wiretap law and subsequent amendments to that piece of legislation.

Let me say at the outset that the Federal wiretap laws have served this country well. They reflect a careful balance between the legitimate needs of law enforcement and the constitutional, guaranteed right of privacy of the individual. Consequently, our laws require law enforcement to obtain a court order based on proof that there is probable cause that a criminal activity is occurring that because of its complex or life-threatening nature necessitates court-sanctioned surveillance.

I should also add that the telecommunications industry has a very good track record of working with law enforcement agencies in effectuating electronic surveillance. There is a substantial and credible record developed over the years by the industry which demonstrates extraordinary effort and cooperation in aiding law enforcement efforts. But we are here today because advances in telecommunications technology have begun to threaten the ability of law enforcement to perform its responsibilities under the Federal wiretap laws.

At a time when all Americans recognize the increased risk associated with crime, as well as the unfettered growth of the crime problem, it is essential that we restore and maintain this critical law enforcement tool. Since this subcommittee has consistently supported policy to accelerate the rapid deployment of new technology, I am pleased that no one has proposed simply freezing technology in place. Rather, the goal of H.R. 4922, the bill we are reviewing today, is to seek to ensure that the capability and capacity needs of law enforcement are satisfied on a contemporaneous basis as the telecommunications network evolves.

As we consider this legislation, I hope we will consider how best to proceed using the careful balancing act set out in all previous Federal wiretap laws by ensuring that all legitimate law enforcement needs are met while the public's legally protected expectation of privacy is also preserved. And I would also add another fact of that, of ensuring that we do not slow technological development and deployment of this particular consideration. They are issues of cost, of speed and demographics of deployment and the scope of coverage that must be considered in that context.

Toward that end, I look forward to hearing our witnesses. And I would also hope that this subcommittee would ask a sequential referral so that we could also look very closely at the legislation. I look forward to the discussion.

I yield back the balance of my time.

Mr. MARKEY. The gentleman's time has expired.

The Chair recognizes the gentleman from Virginia, Mr. Boucher.

Mr. BOUCHER. Thank you very much, Mr. Chairman. Let me say at the outset that I support the passage of legislation that will as-

sure that advances in telecommunications technology do not defeat the ability of law enforcement agencies to engage in authorized wiretaps. Aspects of this legislation, as introduced by Mr. Edwards and referred to the House Judiciary Committee, are clearly within the purview of this committee, and therefore, I commend you, Chairman Markey, for leading an inquiry into certain sensitive and as yet unresolved aspects of the legislation.

Let me be specific about what these various aspects are. First of all, who between the government and the communications industry should bear the cost of the equipment modifications that are going to be required in order to assure that advances in communications technology do not have the effect of defeating the ability of law enforcement to engage in wiretaps? The bill suggests that during the initial transition period of some 4 years, the government should bear that cost, estimated to be about \$500 million. But it is unclear upon whom that cost would fall if either of two events occur: one, the Congress does not provide the appropriation of \$500 million necessary to meet that cost; or two, the ultimate costs of modifying the equipment turn out to be more than the \$500 million estimated. Who then between industry and government would be required to bear that cost?

That ambiguity, in my opinion, should be clearly resolved in favor of those costs falling upon the government for reasons that I will mention in a moment.

The second issue is who should bear those costs after the initial 4-year period? The bill places that responsibility on the industry upon the theory that the costs will be de minimis and insubstantial as these modifications are conveniently designed into succeeding generations of telecommunications equipment. Industry responds that there really is no way of knowing what those ultimate costs are going to be and that, in fact, they could be substantial and significant indeed.

I am persuaded that those costs also should be borne by the government. After all, we are addressing a law enforcement function and just as other law enforcement costs are borne by the agencies and the governments involved, these costs should be borne in precisely the same way. Otherwise, they would fall on telephone company ratepayers, or if it be the industry itself that would satisfy those costs out of profits, then they would come from revenues that we anticipate being spent on advancing the information infrastructure and deploying more capable networks. In either event, I would argue that it is inappropriate for the industry to have to shoulder those costs.

I would say that I also find appealing the argument that is made by the Electronic Frontier Foundation that if government bears these costs, there is greater public accountability and, therefore, more knowledge of wiretapping capability; and that knowledge itself is a very important ingredient of privacy protection.

The third issue, Mr. Chairman, is one of the scope of the bill, and I believe that it should extend not only to the common carriers presently covered and to the mobile telephone service providers currently covered, but also to private networks. There are a number of landlords today of large buildings that are providing internal networks within those structures in order to accommodate the

needs of multiple tenants. These are called shared tenant facilities. As I read the legislation, those kinds of private networks are not covered in the scope of the bill. And that presents a couple of problems.

First of all, I think there is a competitive disadvantage that arises with respect to the covered providers. And second, the law enforcement function is somewhat deterred because the FBI and other agencies would not have the ability to wiretap with respect to those private networks to the same extent that they would with respect to the covered networks. And I think that issue needs to be resolved, and I would suggest that it be resolved in favor of extending the coverage to the private networks as well.

So while I strongly support the passage of the legislation, I think it is essential that we address these outstanding and unresolved concerns, and I look forward to working with the interested parties as we endeavor to do so. Perhaps during the course of this hearing today we can define areas of consensus with respect to these various issues and then those can be incorporated through appropriate amendments, either when the House Judiciary Committee marks up this measure or with a sequential referral to this committee.

Thank you, Mr. Chairman, and I yield back.

Mr. MARKEY. The gentleman's time has expired. The Chair recognizes the gentleman from Ohio, Mr. Oxley.

Mr. OXLEY. Thank you, Mr. Chairman. And let me first congratulate you for the timeliness of this hearing, the importance of our committee in terms of the—if nothing else but the technical aspects of this whole issue; and while we share jurisdiction, hopefully, with the Judiciary Committee, I think our subcommittee certainly has a role to play in this.

Let me also welcome our distinguished panel—panels, really, for being here today. I think this is an excellent opportunity, Mr. Chairman, for the public, through C-Span which is covering this hearing today, to better understand the role of wiretaps in our society, to better understand the essential conflict between trying to protect the right of privacy of all Americans with the equally important aspect of having a strong and effective law enforcement capability, as well.

The authorizing of wiretaps, contrary to some opinions, is not an easy proposition, as I am sure our first panel will point out. There are a lot of hoops that you have to jump through before you can get that authorization. You have to have an affidavit alleging probable cause. You have to have the law enforcement legal eagles scrub that process, whether it is the local prosecutor or the FBI or other law enforcement agencies. You have to have the headquarters, in some cases, go through that, as well. In the Federal case, the Attorney General, the U.S. Attorney's office plays a role, and then ultimately it goes to the magistrate or the Federal judge to seek approval for the wiretap.

So from the public's perception, I think most people don't realize how extremely difficult and time consuming these details are, but they are essential to protect the right of privacy that all Americans should enjoy. And I think, clearly, as you pointed out, Mr. Chairman, our role here is to maintain existing law and not to broaden

the authority of wiretap for law enforcement. Clearly that is not our role, nor is it our goal.

Over the years, we—the courts, the Congress and the State legislatures—have drawn a very delicate balance between that right of privacy and law enforcement, and I think overall we have done a pretty good job of it.

This legislation will facilitate the use of wiretaps in new technology; and essentially what we are trying to do and what law enforcement is trying to do is stay up with the latest technology, which is clearly understandable. So again, I appreciate the timeliness of this hearing.

I have to go to the Rules Committee, but I want to come back and have an opportunity to question the witnesses, because I do think this is an extremely important issue that the more the public understands, I think the more they will appreciate the role of wiretaps and the role of law enforcement in protecting our citizenry.

And I yield back the balance of my time.

Mr. MARKEY. The gentleman's time has expired. While the gentleman didn't mention it, I think it is worth noting that he was an agent for the FBI for many years, and as a member of this Subcommittee on Telecommunications is ideally positioned to understand how a balance could possibly be struck between these two very important interests.

The Chair recognizes the gentleman from Oregon, Mr. Wyden.

Mr. WYDEN. Thank you very much, Mr. Chairman. I want to commend you and Mr. Fields and Mr. Oxley and others who have been dealing with this issue for a long time; and also welcome Director Freeh, who in my view is off to an excellent start in his position as the head of the Bureau.

Mr. Chairman and colleagues, it seems to me that it is important that our law enforcement officials have the tools that they need to deal with the crooks and the thugs in this country that are trying to exploit our citizens. It is essential, however, that these tools of law enforcement be paid for in a forthright and straightforward manner. Therefore, I believe it is essential that a line be drawn in the sand by the Congress early that stipulates there should be no hidden wiretap tax on American consumers.

It is going to be important that law enforcement have the ability to wiretap in instances where there is a risk to the American people, but it must be done and financed in an aboveboard, straightforward fashion. And I am of the view that we need to make modifications in this bill to stipulate that if the appropriations do not come through for enhanced wiretapping, there is to be no mandate that would fall back on the backs of the American consumer.

So I think it is essential that the Bureau has the enhanced wiretapping capability and capacity that it is in a position to pay for. It is, in my view, the best way to make the government accountable. It is the way to ensure that priorities are responsibly set. And it is the way to ensure that hundreds of millions of dollars are not heaped onto the backs of our consumers through some sort of hidden phone tax that is disguised in their monthly telephone bill.

So there is some important work to do.

Mr. Chairman, I would also like to note that Director Freeh visited with myself and other members of the committee on this, and

I think he is very open to working with the Congress on this matter of financing enhanced wiretapping in a responsible way. And I want to associate myself with the remarks that our colleague, Mr. Boucher, made on this point, as well, because I share those in addition.

I yield back.

Mr. MARKEY. The gentleman's time has expired.

The Chair recognizes the gentleman from North Carolina, Mr. McMillan.

Mr. McMILLAN. Thank you, Mr. Chairman.

Like all of us, I have been hearing from my local law enforcement people, as well as here in Washington, about the need to retain our ability to conduct court-authorized wiretaps. I appreciate the concern and wholeheartedly support the efforts to do this.

It has been a valuable tool in law enforcement over the past decade. My information indicates some 22,000 convictions resulting from 8,300 court-approved wiretaps.

I do have some concern about the cost, and I don't know how we are going to resolve this. I believe the FBI is estimating the cost of the program at roughly \$500 million, and the bill mandates that the Federal Government bear that cost over a 4-year period if we get the appropriation from the funds that we all know we don't have. It has been suggested that the industry might then be responsible for bearing the risk of either those funds not being appropriated or the 500 million not being adequate.

I think the statement of the gentleman from Oregon gives me a little concern that we are not going to put this cost on the backs of the consumer, the American taxpayer. Well, if not, who is going to pay for it? You know, companies don't sit out there with a full well of cash to handle this kind of thing. So I think we need to be realistic about that. And I don't know whether it is appropriate to build it into the rate structure or not. That is a pretty good way of distributing it widely over the user system. But I haven't quite come to a conclusion about that. I do think we need to focus both on the quantity and the manner in which we are going to raise it, not back into something that is not funded, that is extremely important to law enforcement efforts.

My other concern has to do with the issue of parity. As I understand it, this legislation is focused on the major regional Bells and independent carriers, and yet we have adopted legislation that would dramatically alter the competitive field for who is going to be providing telephone service to consumers. Therefore, I think anything that we do is going to have to address also the question of an obligation placed upon new competitors in providing service to the traditional system, so that virtually everybody is having to deal with the same obligation insofar as providing access to wiretap.

Those are my two major concerns, and I hope that our witnesses today will cast some light on both those questions.

And I thank the Chair and yield back.

Mr. MARKEY. The gentleman's time has expired.

The Chair now recognizes the gentleman from Illinois, Mr. Hastert.

Mr. HASTERT. I thank the chairman.

Mr. Chairman, I commend you and others for holding this hearing, providing for the rightful review by this subcommittee of wiretapping regulation on common carriers, cellular and PSC providers.

You know, the change to digital from analogue, has certainly opened a lot of new frontiers for telecommunications. It has also challenged us with some problems that we have to address. I think rightly so.

I have to tell you, Director Freeh, that for some of us who you were too busy to talk to, your lieutenants were out there giving us a lot of phone calls. So you have done a good job on the follow-up, and I think that has been helpful. As time grows short in the 103d Congress, this issue is of critical importance to the American people because it impacts the ability of our Nation's crime fighters to do their jobs.

Changing technology brings with it numerous complex issues. Certainly the authority given to the FBI and other law enforcement officials in the 1967 Federal wiretap law, as amended in 1986 by the Electronic Communications Privacy Act, to seek court orders to wiretap when a court order has been issued, must be maintained. We should not neglect the pervading public interest in retaining this wiretapping authority simply because technology is changing.

We will hear testimony as to the cost of developing the capability and increasing the capacity for law enforcement officials to conduct legal wiretaps in our Nation's communications networks. This will be very interesting to me, as I believe the question of who bears the cost for changes to the system is a central issue.

I believe we may all be able to concede that this issue must be faced soon. If all parties involved cannot find an acceptable and fair agreement, the use of an important crime-fighting tool will be significantly impeded. Yet, if I might more accurately say when—the cost of modifying our Nation's communications networks exceeds the \$500 million included in the legislation currently being considered by the Judiciary Committee, who will be left holding the bill?

I understand the parties involved have come a long way in their thinking in the last few years. However, I look forward to your comments on how this issue of cost and other related issues, such as the need for prioritization and the scope of covered networks, can and should be resolved.

Thank you, Mr. Chairman.

Mr. MARKEY. The gentleman's time has expired.

Now we will hear from the ranking minority member of the full committee, the gentleman from California, Mr. Moorhead.

Mr. MOORHEAD. Thank you, Mr. Chairman. I want to commend you for calling today's hearing on this important issue of requiring wiretapping capability in the telecommunications network.

It is critical that we ensure that law enforcement has the tools necessary to perform its duties. As the network evolves, criminals become more sophisticated along the line in using it. Congress has provided law enforcement with the means of fighting crime through electronic surveillance in the past. In 1967, Federal wiretap law set the original ground rules. That law has been amended to reflect changes in technology in the network, most notably, the 1986 Electronics Communications Privacy Act, which I cosponsored, updated the Federal wiretap law in numerous critical ways.

We are now at another critical stage in the development of the telecommunications network and the ability of law enforcement to carry out its responsibilities in the light of it. I am confident that industry and law enforcement will again be able to work together to solve the new issues posed today. I look forward to the testimony as we embark on that course of action.

Thank you, Mr. Chairman.

Mr. MARKEY. The gentleman's time has expired.

There are no other members seeking recognition for the purpose of making an opening statement at this time. We will turn to our first panel, and we will begin by recognizing the Honorable Louis Freeh, who is the Director of the Federal Bureau of Investigation. Mr. Freeh is a former FBI agent, former Federal judge, extremely well qualified to speak to all aspects of this issue.

We welcome you to the subcommittee, sir. Whenever you feel comfortable, please begin.

STATEMENTS OF HON. LOUIS J. FREEH, DIRECTOR, FEDERAL BUREAU OF INVESTIGATION; THOMAS REILLY, DISTRICT ATTORNEY, MIDDLESEX COUNTY, CAMBRIDGE, MA.; AND A. RICHARD METZGER, DEPUTY CHIEF, COMMON CARRIER BUREAU, FEDERAL COMMUNICATIONS COMMISSION

Mr. FREEH. Thank you, Chairman Markey.

Mr. MARKEY. If you could, please turn on the microphone.

Mr. FREEH. Thank you, Chairman Markey, Congressman Fields, other distinguished members of the panel. It is a great privilege to have my first appearance before this distinguished committee.

I would like to use my time briefly to highlight some of the critical issues relating to the digital telephony problem. Many of the members have just correctly pointed to some of the remaining issues that need to be addressed.

Today, as we all know, the crime bill was signed, which has in its contemplation the deployment of 100,000 new police officers to cities and towns around the United States. What we are asking to have maintained, which is the access we now have pursuant to court order to conversations of people who violate our criminal laws and threaten our national security, is exactly what is at stake.

The officers who will be deployed under the crime bill will need the necessary tools to do their job. On a Federal level, taking away a tool that is as critical as electronic surveillance would be the equivalent of sending a road officer or a city officer into the streets without one of his pouches of ammunition. It is that critical to the work that is done.

We have made great progress with the industry, with the committee and this staff, the other staffs involved, over a long period of time, and are very anxious to bring this important matter to closure.

As you know, on March 18, I testified before a joint hearing of the House and Senate Judiciary Subcommittees, and I will enclose a copy of that testimony for the record with your permission.

Mr. MARKEY. Without objection, it will be included in the record.
[The information follows:]

STATEMENT
OF
LOUIS J. FREEH
DIRECTOR
FEDERAL BUREAU OF INVESTIGATION
WASHINGTON, D.C.
MARCH 18, 1994
BEFORE THE
SUBCOMMITTEE ON TECHNOLOGY AND THE LAW
OF THE COMMITTEE ON THE JUDICIARY
UNITED STATES SENATE
AND THE
SUBCOMMITTEE ON CIVIL AND CONSTITUTIONAL RIGHTS
OF THE COMMITTEE ON THE JUDICIARY
HOUSE OF REPRESENTATIVES

MR. CHAIRMEN, I APPRECIATE THE OPPORTUNITY TO APPEAR BEFORE YOUR SUBCOMMITTEES. I AM HERE TODAY NOT JUST IN MY CAPACITY AS DIRECTOR OF THE FEDERAL BUREAU OF INVESTIGATION BUT ALSO AS A SPOKESMAN FOR OUR NATION'S LAW ENFORCEMENT AND INTELLIGENCE COMMUNITIES REGARDING A MATTER OF EXTREME URGENCY AND IMPORTANCE. I AM HERE ON BEHALF OF THE ADMINISTRATION TO TELL YOU THAT WE ARE CONFRONTED WITH A MAJOR THREAT TO OUR ABILITY TO PROTECT THE AMERICAN PUBLIC, SAFEGUARD THE NATIONAL SECURITY, AND EFFECTIVELY ENFORCE THE LAW. THIS THREAT RESULTS FROM VARIOUS TECHNOLOGICAL IMPEDIMENTS TO OUR ABILITY TO EXECUTE COURT ORDERS AND LAWFULLY CONDUCT ELECTRONIC SURVEILLANCE AND ACQUIRE THE ASSOCIATED DIALING INFORMATION. THESE IMPEDIMENTS ARE THE UNINTENDED SIDE EFFECTS OF ADVANCED TELECOMMUNICATIONS TECHNOLOGY WHICH HAS BEEN, AND CONTINUES TO BE, DEPLOYED WITHOUT CONSIDERATION FOR THE CRITICAL NEEDS OF OUR NATION'S LAW ENFORCEMENT AND INTELLIGENCE AGENCIES.

I AM HERE TODAY TO STRONGLY ASSERT WHAT I AND THE ADMINISTRATION BELIEVE IS THE ONLY RATIONAL AND VIABLE MEANS OF REMOVING THIS THREAT -- THE ENACTMENT OF THE PROPOSED

COMPREHENSIVE LEGISLATION TO ADDRESS THE DIGITAL TELEPHONY ISSUE. WITHOUT ITS ENACTMENT, ONE OF OUR MOST EFFECTIVE WEAPONS AGAINST NATIONAL AND INTERNATIONAL DRUG TRAFFICKING, TERRORISM, ESPIONAGE, ORGANIZED CRIME, AND SERIOUS VIOLENT CRIMES WILL BE SEVERELY AND ADVERSELY IMPACTED.

THE ADMINISTRATION WANTS TO WORK WITH THE CONGRESS TO DEVELOP SUCH COMPREHENSIVE LEGISLATION. I WILL DESCRIBE IN THIS TESTIMONY A DRAFT LEGISLATIVE PROPOSAL THAT HAS BEEN SHARED WITH YOU.

QUITE SIMPLY, THE PURPOSE OF THIS LEGISLATION (DRAFT) IS TO MAINTAIN TECHNOLOGICAL CAPABILITIES COMMENSURATE WITH EXISTING STATUTORY AUTHORITY -- THAT IS, TO PREVENT ADVANCED TELECOMMUNICATIONS TECHNOLOGY FROM REPEALING DE FACTO THE STATUTORY AUTHORITY ALREADY CONFERRED BY THE CONGRESS. THE PROPOSED LEGISLATION EXPLICITLY STATES THAT THE LEGISLATION DOES NOT ENLARGE OR REDUCE THE GOVERNMENT'S AUTHORITY TO LAWFULLY CONDUCT COURT-ORDERED ELECTRONIC SURVEILLANCE AND INSTALL OR USE COURT-ORDERED PEN REGISTER OR TRAP AND TRACE DEVICES. THE ESSENCE OF THE DRAFT LEGISLATION IS TO CLARIFY AND MORE FULLY DEFINE THE NATURE AND EXTENT OF THE TELECOMMUNICATIONS SERVICE PROVIDER'S "ASSISTANCE" REQUIREMENT THAT WAS ENACTED BY CONGRESS IN 1970. THAT REQUIREMENT EVIDENCED CONGRESS' CLEAR INTENT THAT LAWFUL COURT ORDERS SHOULD NOT BE FRUSTRATED DUE TO A SERVICE PROVIDER'S FAILURE TO PROVIDE NEEDED TECHNOLOGICAL ASSISTANCE AND FACILITIES. THE PROPOSED LEGISLATION RELATES SOLELY TO ADVANCED TECHNOLOGY, NOT LEGAL AUTHORITY OR PRIVACY.

WE DID NOT COME TO SEEK LEGISLATION BLITHELY. FOR NEARLY FOUR YEARS, THE FBI HAS EXPENDED EVERY REASONABLE EFFORT TO ADDRESS THIS THREAT THROUGH NUMEROUS AND ONGOING MEETINGS WITH THE TELECOMMUNICATIONS INDUSTRY. HOWEVER, IT IS MY CONSIDERED JUDGEMENT, AND THAT OF THE ADMINISTRATION, THAT DIALOGUE ALONE, NO MATTER HOW WELL INTENDED, WILL NOT SOLVE THIS SERIOUS THREAT TO PUBLIC SAFETY. NONETHELESS, WE HAVE LISTENED AND LEARNED, AND THE LEGISLATIVE PROPOSAL BEFORE YOU REPRESENTS, IN OUR ESTIMATION, THE ONLY PROPER APPROACH. ON THE ONE HAND, IT DEALS

WITH THE ADVANCED TELEPHONY PROBLEM IN AN APPROPRIATELY COMPREHENSIVE FASHION -- IT DOES NOT SIMPLY "BAND-AID-OVER" PAST PROBLEMS, IT ALSO RESPONSIBLY DEALS WITH NEW SERVICES AND TECHNOLOGIES (SUCH AS PERSONAL COMMUNICATIONS SERVICES) THAT LIKELY WILL EMERGE IN THE NEXT FEW YEARS. ON THE OTHER HAND, THE DRAFT LEGISLATION IS NARROWLY FOCUSED AND COVERS ON ONLY THOSE SEGMENTS OF THE TELECOMMUNICATIONS INDUSTRY WHERE THE VAST MAJORITY OF THE PROBLEMS EXIST -- THAT IS, ON COMMON CARRIERS, A SEGMENT OF THE INDUSTRY WHICH HISTORICALLY HAS BEEN SUBJECT TO REGULATION. WE BELIEVE THE PROVISIONS OF THE ADMINISTRATION'S PROPOSAL ADDRESS THE PROBLEM IN A VERY RATIONAL FASHION. THEY INCLUDE CLEARLY STATED LAW ENFORCEMENT ELECTRONIC SURVEILLANCE REQUIREMENTS, SYSTEMS SECURITY PROVISIONS, A REASONABLE DEADLINE FOR COMPLIANCE, REQUIREMENTS FOR EQUIPMENT MANUFACTURER AND SUPPORT SERVICE PROVIDER COOPERATION, PROPER ENFORCEMENT AND PENALTY PROVISIONS, ONGOING GOVERNMENT CONSULTATION WITH COMMON CARRIERS TO FACILITATE COMPLIANCE, AND, IMPORTANTLY, A COMMITMENT ON THE PART OF THE FEDERAL GOVERNMENT TO PAY COMMON CARRIERS FOR REASONABLE CHARGES ASSOCIATED WITH ACHIEVING COMPLIANCE.

IMPORTANCE OF ELECTRONIC SURVEILLANCE

AS THE PROPOSED LEGISLATION IS CONSIDERED, IT IS ABSOLUTELY ESSENTIAL THAT CONGRESS UNDERSTAND THE IMPORTANCE OF ELECTRONIC SURVEILLANCE, AS WELL AS THE SEVERE HARM THAT WILL OCCUR IF THIS CRITICAL LAW ENFORCEMENT TOOL IS LOST OR DIMINISHED.

THE NATION'S TELECOMMUNICATIONS NETWORKS ARE ROUTINELY USED IN THE COMMISSION OF SERIOUS CRIMINAL ACTIVITIES, INCLUDING TERRORISM AND ESPIONAGE. ORGANIZED CRIME GROUPS AND DRUG TRAFFICKING ORGANIZATIONS, WHICH ARE OFTEN HIGHLY STRUCTURED, RELY HEAVILY UPON TELECOMMUNICATIONS TO PLAN AND EXECUTE THEIR CRIMINAL ACTIVITIES AND HIDE THEIR ILLEGAL PROCEEDS. SIMILARLY, FOREIGN INTELLIGENCE SERVICE OFFICERS AND THEIR AGENTS CARRY OUT THEIR SPY AND OTHER CLANDESTINE MISSIONS THROUGH THESE NETWORKS.

CONGRESS RECOGNIZED THIS FACT A LITTLE OVER 25 YEARS AGO, WHEN IT PASSED THE OMNIBUS CRIME CONTROL AND SAFE STREETS ACT OF 1968. TITLE III OF THAT ACT CONTAINED THE FIRST COMPREHENSIVE FEDERAL LEGISLATIVE REGIMEN REGARDING ELECTRONIC SURVEILLANCE FOR USE IN CRIMINAL INVESTIGATIONS. THE TITLE III LEGISLATION ESTABLISHED STRICT PROCEDURES FOR THE CONDUCT OF ELECTRONIC SURVEILLANCE BY FEDERAL, STATE AND LOCAL LAW ENFORCEMENT AUTHORITIES. THESE PROCEDURES ARE CAREFULLY ADHERED TO BY LAW ENFORCEMENT AND ARE RIGOROUSLY ENFORCED BY THE COURTS. TO DATE, THIRTY-SEVEN (37) STATES, PUERTO RICO, THE U.S. VIRGIN ISLANDS, AND THE DISTRICT OF COLUMBIA ALSO HAVE ENACTED ELECTRONIC SURVEILLANCE STATUTES. IN 1992, A TOTAL OF 919 TITLE III ORDERS, AS WELL AS AN ESTIMATED 9,000 PEN REGISTER ORDERS, WERE AUTHORIZED FOR ALL FEDERAL, STATE, AND LOCAL LAW ENFORCEMENT AGENCIES. ON AVERAGE, APPROXIMATELY TWO-THIRDS OF THE CRIMINAL-RELATED ELECTRONIC SURVEILLANCE CONDUCTED IN THE UNITED STATES IS CARRIED OUT BY STATE AND LOCAL LAW ENFORCEMENT AGENCIES. AS MANDATED IN THE TITLE III LEGISLATION, ELECTRONIC SURVEILLANCE MAY BE USED ONLY IN THE INVESTIGATION OF SERIOUS FELONY OFFENSES AND ONLY WHEN OTHER INVESTIGATIVE TECHNIQUES WILL NOT WORK OR ARE TOO DANGEROUS.

IN 1978, CONGRESS ESTABLISHED AN ANALOGOUS FEDERAL ELECTRONIC SURVEILLANCE REGIMEN FOR USE IN COUNTER-INTELLIGENCE, COUNTER-TERRORISM, AND COUNTER-ESPIONAGE INVESTIGATIONS, THE FOREIGN INTELLIGENCE SURVEILLANCE ACT OF 1978 (FISA). PURSUANT TO FISA, THE U. S. GOVERNMENT IS AUTHORIZED TO INTERCEPT COMMUNICATIONS OF INDIVIDUALS WHO POSE A THREAT TO THE NATIONAL SECURITY, AND INCLUDE THOSE IN FURTHERANCE OF ESPIONAGE AND TERRORISM.

SINCE THE PASSAGE OF TITLE III, LAW ENFORCEMENT HAS FOUND ELECTRONIC SURVEILLANCE TO BE ONE OF ITS MOST IMPORTANT INVESTIGATIVE TECHNIQUES -- IF NOT THE MOST IMPORTANT. USE OF THE TECHNIQUE HAS BEEN CRITICAL IN FIGHTING ORGANIZED CRIME, DRUG TRAFFICKING, PUBLIC CORRUPTION, FRAUD, TERRORISM, AND VIOLENT CRIME, AND IN SAVING NUMEROUS INNOCENT LIVES. IN MANY OF THESE

CASES, THE CRIMINAL ACTIVITY UNDER INVESTIGATION COULD NEVER HAVE BEEN FULLY DETECTED, PREVENTED, ADEQUATELY INVESTIGATED, OR SUCCESSFULLY PROSECUTED WITHOUT THE USE OF EVIDENCE DERIVED FROM COURT-ORDERED ELECTRONIC SURVEILLANCE. SIMILARLY, FISA-BASED INTELLIGENCE INFORMATION MAKES A SIGNIFICANT AND IMPORTANT CONTRIBUTION TO U. S. COUNTER-INTELLIGENCE, COUNTER-TERRORISM, AND COUNTER-ESPIONAGE EFFORTS.

AS YOU ARE AWARE, ELECTRONIC SURVEILLANCE IS A CRITICAL TOOL USED TO DETECT AND OBTAIN EVIDENCE OF, AND OFTEN PREVENT, THE MOST SERIOUS, AND OFTEN MOST VIOLENT, CRIMINAL ACTIVITY CONFRONTING OUR SOCIETY. AS SHOWN IN THE ATTACHED EXHIBIT, ALTHOUGH USED SPARINGLY, ELECTRONIC SURVEILLANCE HAS PROVED TO BE AN EXTREMELY EFFECTIVE INVESTIGATIVE TECHNIQUE FOR LAW ENFORCEMENT AND HAS LED TO THE CONVICTIONS OF THOUSANDS OF DANGEROUS PERSONS INVOLVED IN DRUG TRAFFICKING, ORGANIZED CRIME, VIOLENT CRIME, KIDNAPING, CRIMES AGAINST CHILDREN, AND PUBLIC CORRUPTION. BECAUSE A SUBSTANTIAL NUMBER OF PROSECUTIONS ARE ONGOING, THE EXACT NUMBER OF CONVICTIONS RESULTING FROM THESE WIRETAPS INCREASES ALMOST DAILY; HOWEVER, THIS KEY INVESTIGATIVE TECHNIQUE HAS PROVEN TO BE INCOMPARABLY EFFECTIVE, WITH THE RESULTING EVIDENCE SECURING THE CONVICTION OF OVER 22,000 DANGEROUS FELONS OVER THE PAST DECADE.

PUBLIC SAFETY: PREVENTING CRIMES AND SAVING HUMAN LIVES

ALTHOUGH ELECTRONIC SURVEILLANCE IS EXTREMELY IMPORTANT AS AN INVESTIGATIVE TOOL TO ACQUIRE EVIDENCE, FREQUENTLY IT HAS BEEN ESSENTIAL IN PREVENTING CRIMES FROM OCCURRING AND IN SAVING HUMAN LIFE. ELECTRONIC SURVEILLANCE HAS BEEN ESSENTIAL IN PREVENTING MURDERS; IN SAVING HUMAN LIFE PUT AT RISK THROUGH PLANNED TERRORIST ATTACKS; IN DISMANTLING ENTRENCHED ORGANIZED CRIME GROUPS WHICH SEVERELY HARM THE ECONOMY THROUGH EXTORTION, FRAUD, AND CORRUPTION; AND IN ATTACKING THE MAJOR NATIONAL AND INTERNATIONAL DRUG IMPORTATION AND DISTRIBUTION CARTELS AND NETWORKS WHOSE ACTIVITIES RAVAGE SOCIETY AND CAUSE INCALCULABLE PERSONAL AND ECONOMIC INJURY IN THE UNITED STATES.

ORGANIZED CRIME INVESTIGATIONS

THE ACTIVITIES OF ORGANIZED CRIME ARE EXTREMELY HARMFUL TO AMERICAN BUSINESS AND INDUSTRY, LABOR UNIONS, AND INDIVIDUALS IN OUR SOCIETY. ELECTRONIC SURVEILLANCE IS INDISPENSABLE IN COMBATTING ORGANIZED CRIME. INDEED, THE FBI'S ORGANIZED CRIME/DRUGS SECTION REPORTS THAT EVERY MAJOR FBI ORGANIZED CRIME INVESTIGATION HAS RELIED UPON ELECTRONIC SURVEILLANCE. IN APRIL, 1988, THE IMPORTANCE OF THE ELECTRONIC SURVEILLANCE TECHNIQUE WAS FORMALLY RECOGNIZED IN HEARING TESTIMONY BEFORE THE U.S.. SENATE PERMANENT SUBCOMMITTEE ON INVESTIGATIONS, GOVERNMENTAL AFFAIRS COMMITTEE, ON ORGANIZED CRIME: "25 YEARS AFTER VALACHI." IN PARTICULAR, DAVID C. WILLIAMS, OFFICE OF SPECIAL INVESTIGATIONS, GENERAL ACCOUNTING OFFICE, TESTIFIED THAT "ELECTRONIC SURVEILLANCE IS ANOTHER TOOL THAT HAS BEEN OF GREAT VALUE TO THE LAW ENFORCEMENT COMMUNITY TO COMBAT THE LA COSA NOSTRA (LCN) [ORGANIZED CRIME FAMILIES]. EVIDENCE GATHERED THROUGH ELECTRONIC SURVEILLANCE ... HAS HAD A DEVASTATING IMPACT ON ORGANIZED CRIME." (EMPHASIS ADDED)

LEFT UNCHECKED, ORGANIZED CRIME EXERTS A CHOKE HOLD ON SOCIETY, AND THE SUBSEQUENT COST TO BUSINESS AND INDUSTRY IS DRAMATIC. GREATER DETAIL CONCERNING AREAS OF ORGANIZED CRIME'S PENETRATION IN BUSINESS AND LABOR UNIONS AND EXAMPLES OF THE SUCCESSFUL USE OF ELECTRONIC SURVEILLANCE TO EFFECTIVELY COMBAT THE ADVERSE IMPACT OF ORGANIZED CRIME UPON THE ECONOMY AND SOCIETY IS SET FORTH IN THE ATTACHED APPENDIX.

IN THE 1986 REPORT, THE IMPACT: ORGANIZED CRIME TODAY, THE PRESIDENT'S COMMISSION ON ORGANIZED CRIME UTILIZED THE WHARTON BUSINESS SCHOOL'S LONG-TERM MODEL OF THE UNITED STATES ECONOMY TO ESTIMATE THE COST OF ORGANIZED CRIME ON THE ECONOMY, IN TERMS OF SUSTAINED HIGHER PRICES AND THE CONTINUED UNDERPAYMENT OF TAXES TO THE FEDERAL GOVERNMENT. THE COMMISSION CONCLUDED THAT THE ESTIMATED ECONOMY-WIDE IMPACT OF ORGANIZED CRIME, EXCLUDING DRUG TRAFFICKING ORGANIZATIONS, WAS AS FOLLOWS:

O U. S. OUTPUT WAS REDUCED BY \$18.2 BILLION IN 1986 DOLLARS.

- O U. S. EMPLOYMENT WAS REDUCED BY 414,000 JOBS.
- O CONSUMER PRICES WERE HIGHER BY 0.3 PERCENT; AND,
- O PER CAPITA PERSONAL INCOME WAS LOWER BY \$77.22, MEASURED IN 1986 DOLLARS.

FBI ORGANIZED CRIME PROGRAM MANAGERS STATE: "THE LOSS OR IMPAIRMENT OF THE CAPABILITY TO CONDUCT COURT-ORDERED ELECTRONIC SURVEILLANCE WOULD CATASTROPHICALLY IMPAIR FEDERAL AND STATE LAW ENFORCEMENT AGENCIES' ABILITY TO EFFECTIVELY INVESTIGATE ORGANIZED CRIMINAL GROUPS." (EMPHASIS ADDED)

ALTHOUGH NO STUDIES HAVE BEEN CONDUCTED TO MEASURE THE PRECISE ECONOMIC AND SOCIETAL BENEFITS DERIVED FROM THE SUCCESSES OF FEDERAL AND STATE CRIMINAL LAW ENFORCEMENT AGENCIES AGAINST ORGANIZED CRIME, IT IS EVIDENT THAT AN ABATEMENT IN SUCCESSFUL ORGANIZED CRIME INVESTIGATIONS, DUE TO THE LOSS OR IMPAIRMENT OF ONE OF LAW ENFORCEMENT'S MOST IMPORTANT TOOLS -- THE COURT-ORDERED ELECTRONIC SURVEILLANCE TECHNIQUE -- WOULD ALLOW ORGANIZED CRIME'S DAMAGE TO THE U.S. ECONOMY TO BECOME SUBSTANTIALLY GREATER.

NARCOTICS AND DANGEROUS DRUGS

THE GREATEST USE OF ELECTRONIC SURVEILLANCE BY LAW ENFORCEMENT RELATES TO THE FEDERAL AND STATE GOVERNMENTS' "WAR ON DRUGS." INFORMATION REPORTED IN THE FEDERAL WIRETAP REPORT BY THE ADMINISTRATIVE OFFICE OF THE UNITED STATES COURTS INDICATES THAT ALMOST TWO THIRDS (62%) OF ALL TITLE III GOVERNMENTAL ELECTRONIC SURVEILLANCE IS DEVOTED TO THIS CRITICAL NATIONAL PROBLEM. THE MAJOR DRUG TRAFFICKING ORGANIZATIONS WHICH IMPORT AND DISTRIBUTE DRUGS, LIKE ANY BUSINESS OR ORGANIZATION, RELY HEAVILY ON TELECOMMUNICATIONS TO COORDINATE AND CARRY OUT THESE CRIMINAL ACTIVITIES AND TO "LAUNDER" THE BILLIONS OF DOLLARS IN ILLEGAL DRUG PROCEEDS. ACCORDINGLY, FEDERAL AND STATE LAW ENFORCEMENT MAXIMIZE THEIR LIMITED RESOURCES AND FOCUS ELECTRONIC SURVEILLANCE EFFORTS ON THE MAIN DRUG IMPORTATION AND DISTRIBUTION NETWORKS.

ALTHOUGH FIGURES ABOUND WITH REGARD TO THE BILLIONS OF

DOLLARS IN FEDERAL, STATE, AND LOCAL SEIZURES OF DRUGS, ILLEGAL DRUG PROCEEDS (CASH AND OTHER ASSETS), ETC., THE FUNDAMENTAL HARM TO SOCIETY IS INCALCULABLE. IT IS IMPOSSIBLE TO FULLY IDENTIFY THE HUMAN, ECONOMIC, AND OTHER SOCIETAL HARM BROUGHT ABOUT BY DRUG DEPENDENCY AND ADDICTION. IN ONE ATTEMPT TO QUANTIFY CERTAIN FACETS OF THIS HARM, THE U. S. PUBLIC HEALTH SERVICE HAS ESTIMATED THE HEALTH, LABOR, AND CRIME COSTS OF DRUG ABUSE AT \$58.3 BILLION IN 1988, EXCLUSIVE OF THE VALUE OF THE DRUGS THEMSELVES. D. RICE, ET AL., U. S. DEPARTMENT OF HEALTH AND HUMAN SERVICES, THE ECONOMIC COST OF ALCOHOL AND DRUG ABUSE AND MENTAL ILLNESS: 1985, TABLE 1, PAGE 2 (1990). A 1992 U. S. DEPARTMENT OF HEALTH AND HUMAN SERVICES' STUDY ESTIMATES THE 1992 COSTS OF DRUG ABUSE IN THE UNITED STATES TO BE \$168 BILLION OR \$675 PER PERSON. APPROXIMATELY \$40 BILLION DOLLARS A YEAR ARE SPENT BY USERS TO PROCURE THESE DRUGS.

ULTIMATELY, THE ECONOMIC, SOCIETAL, AND PERSONAL HARM OF DRUG TRAFFICKING IS ALSO MEASURED IN DAILY "DRIVE-BY SHOOTINGS" IN NEIGHBORHOOD STREETS (WHERE THE BLOOD OF INNOCENT CHILDREN IS SPILLED NEXT TO THAT OF NEIGHBORHOOD DRUG LIEUTENANTS); SUBSTANTIALLY INCREASED CRIME SUCH AS THEFTS, ROBBERIES, AND MURDERS BROUGHT ABOUT BY DRUG USE; VIOLENT "TURF BATTLES" TO CONTROL DRUG DISTRIBUTION; LOST PRODUCTIVITY; EMPLOYEE ABSENCE; EXTENSIVE AND EXPENSIVE HEALTH CARE WITH DRUG CASUALTIES THAT CLOG OUR HOSPITAL EMERGENCY ROOMS; AS WELL AS THE SAD OCCURRENCE OF A GENERATION OF DRUG-DEPENDANT BABIES.

THE DRUGS WHICH ARE MOST RESPONSIBLE FOR THIS PROBLEM ARE ESSENTIALLY THOSE (SUCH AS COCAINE AND HEROIN) WHICH MUST BE IMPORTED INTO THE UNITED STATES, GENERALLY BY HIGHLY ORGANIZED CRIMINAL GROUPS, DRUG TRAFFICKING CARTELS AND OTHER SYNDICATES, AND THEREAFTER TRANSPORTED OVER VAST DISTANCES AND DISTRIBUTED WIDELY WITHIN THE UNITED STATES. THESE CARTELS AND ORGANIZATIONS RELY HEAVILY ON TELECOMMUNICATIONS TO CARRY OUT THEIR ILLEGAL ACTIVITIES. THE UNITED STATES GOVERNMENT ESTIMATES THAT EVERY YEAR OVER 400 METRIC TONS OF COCAINE AND APPROXIMATELY 18 TO 22 METRIC TONS OF HEROIN ARE SMUGGLED INTO THE UNITED STATES.

ELECTRONIC SURVEILLANCE IS CRITICAL IN THE MONITORING OF THE DRUG TRAFFICKERS' "COMMUNICATIONS NETWORKS," PROVIDING LAW ENFORCEMENT WITH THE ABILITY TO IDENTIFY ALL OF THE ORGANIZATION'S DRUG TRAFFICKERS AND THEIR ILLEGAL PROCEEDS, AS WELL AS ULTIMATELY IN DISMANTLING THOSE NATIONAL AND INTERNATIONAL DRUG TRAFFICKING ORGANIZATIONS. SINCE NATIONAL AND INTERNATIONAL DRUG CHIEFTAINS AND LOCAL DRUG "KINGPINS" DO NOT APPEAR AT DRUG BUYS OR SHIPMENTS, ELECTRONIC SURVEILLANCE ORDINARILY PROVIDES THE ONLY RELIABLE METHOD OF LINKING THE DRUG ORGANIZATIONS' LEADERS WITH THE ENTERPRISE, AND FREQUENTLY PROVIDES THE ONLY DIRECT AND PERSUASIVE EVIDENCE THAT WILL SUPPORT A CRIMINAL CONVICTION. CONSEQUENTLY, INFORMATION DERIVED FROM ELECTRONIC SURVEILLANCE IS ESSENTIAL IN SUCCESSFULLY PROSECUTING THOSE AT THE EXECUTIVE LEVEL OF THE DRUG TRADE.

RECENT EXAMPLES OF THE CRITICAL ROLE OF ELECTRONIC SURVEILLANCE IN DRUG INVESTIGATIONS ARE:

- O IN A NEW YORK CITY-BASED DRUG TRAFFICKING INVESTIGATION, AN FBI-LED TASK FORCE CONDUCTED OVER 55 SEPARATE ELECTRONIC SURVEILLANCES (WITH NUMEROUS EXTENSIONS). AS OF MARCH 1993, THIS INVESTIGATION HAS RESULTED IN 222 ARRESTS; 167 CONVICTIONS; THE DISMANTLING OF 15 MAJOR DRUG TRAFFICKING ORGANIZATIONS/GANGS, AND THE IDENTIFICATION OF 30 OTHERS; THE RESOLUTION OF SOME 40 NEW YORK AREA HOMICIDES, INCLUDING THE ASSASSINATION OF A NYCPD POLICE OFFICER AND A NEW YORK STATE PAROLE OFFICER. SUBSTANTIAL QUANTITIES OF DRUGS HAVE BEEN SEIZED AND OVER \$8 MILLION IN ASSETS HAVE BEEN SEIZED. THESE EFFORTS HAVE RESULTED IN A SUBSTANTIAL REDUCTION IN DRUG-RELATED HOMICIDES.
- O THE APRIL, 1992, DRUG RAID IN MIAMI THAT NETTED 15,000 POUNDS OF COCAINE WHICH WAS BASED ON INFORMATION DEVELOPED THROUGH ELECTRONIC SURVEILLANCE. EVIDENCE DERIVED FROM ELECTRONIC SURVEILLANCE WAS INSTRUMENTAL

IN IDENTIFYING THE NETWORK'S LEADER AMONG THE 22
DEFENDANTS ARRESTED;

- O THE 1991 DEA HERRERA DRUG INVESTIGATION IN NEW YORK
CITY RESULTING IN THE SUCCESSFUL PROSECUTION OF 51
DEFENDANTS, INCLUDING KEY INDIVIDUALS LINKED TO THE
CALI DRUG CARTEL, RELIED UPON ELECTRONIC SURVEILLANCE.

WITHOUT THE USE OF ONE OF FEDERAL AND STATE LAW
ENFORCEMENT'S MOST IMPORTANT ENFORCEMENT TOOLS -- ELECTRONIC
SURVEILLANCE -- THE VOLUME OF DRUGS WOULD DRAMATICALLY INCREASE
AND THE EASE AND MEANS OF DRUG IMPORTATION AND DISTRIBUTION WOULD
BE DRAMATICALLY ENHANCED THROUGH THE DRUG TRAFFICKERS' UNFETTERED
USE OF THEIR DRUG "COMMUNICATIONS NETWORKS."

PUBLIC CORRUPTION AND GOVERNMENTAL FRAUD

INTEGRITY IN GOVERNMENT IS A KEYSTONE IN ANY DEMOCRACY.
CORRUPTION AND FRAUD UNDERMINE THE PUBLIC'S RESPECT AND
CONFIDENCE IN GOVERNMENTAL INSTITUTIONS AND IN THE RULE OF LAW.
BY THEIR NATURE, CORRUPTION AND FRAUD CAN ONLY FLOURISH IN
SECRECY, HIDDEN FROM PUBLIC VIEW. AS A RESULT, NORMAL, OVERT
INVESTIGATIVE TECHNIQUES ARE IN MOST CASES TOTALLY UNAVAILING.
HENCE, AS A GENERAL PROPOSITION, LAW ENFORCEMENT HAS FOUND THAT
ELECTRONIC SURVEILLANCE AND UNDERCOVER OPERATIONS ARE CRITICAL
MEANS TO EFFECTIVELY DETECT, INVESTIGATE, AND PROSECUTE THESE
INSIDIOUS CRIME PROBLEMS.

IN SEVERAL RECENT JUDICIAL CORRUPTION INVESTIGATIONS,
ELECTRONIC SURVEILLANCE EVIDENCE HAS DIRECTLY LED TO THE
CONVICTION OF TWO FEDERAL DISTRICT COURT JUDGES AND, IN ANOTHER
CASE, TO THE INDICTMENT OR PLEA OF SIX CURRENT OR FORMER DADE
COUNTY, FLORIDA, STATE JUDGES (FOUR CONVICTED, ONE ACQUITTED, AND
ONE TO BE RETRIED) AND FIVE ATTORNEYS (ALL CONVICTED) FOR
EXTORTION AND CASE FIXING. WITHIN THE RECENT PAST, ELECTRONIC
SURVEILLANCE HELPED BUILD A CORRUPTION CASE INVOLVING THE POLICE
FORCE OF A LARGE MIDWESTERN CITY WHICH INCLUDED EXTORTION AND

PROTECTION FOR GAMBLING AND NARCOTICS DISTRIBUTION. THIRTY POLICE OFFICERS AND 17 OTHERS WERE INDICTED, AND 46 OF THE 47 EITHER PLED OR HAVE BEEN FOUND GUILTY.

ELECTRONIC SURVEILLANCE HAS PLAYED AN INDISPENSABLE ROLE IN COUNTERING GOVERNMENTAL FRAUD. FOR EXAMPLE, THE "ILL-WIND" INVESTIGATION (WHICH WAS LARGELY BASED UPON 36 SEPARATE COURT-ORDERED ELECTRONIC SURVEILLANCES CONDUCTED ACROSS THE UNITED STATES) HAS HAD A TREMENDOUS IMPACT UPON FRAUD AND ABUSE BOTH WITHIN THE GOVERNMENT AND WITHIN THE INDUSTRIES THAT CONTRACT WITH THE GOVERNMENT. TO DATE, THE "ILL-WIND" INVESTIGATION HAS RESULTED IN 65 CONVICTIONS (INCLUDING HIGH-LEVEL DEPARTMENT OF DEFENSE OFFICIALS AND EIGHT CORPORATIONS), SANCTIONS AGAINST CONTRACTORS, AND OVER A QUARTER OF A BILLION DOLLARS (\$271,000,000) IN FINES, RESTITUTIONS, AND RECOVERIES ORDERED. EVIDENCE NECESSARY TO OBTAIN THESE CONVICTIONS, FINES, RECOVERIES, ETC., WOULD HAVE BEEN IMPOSSIBLE TO OBTAIN WITHOUT ELECTRONIC SURVEILLANCE.

THE HIGH COST OF HEALTH CARE IN THE UNITED STATES IS A PROBLEM OF TREMENDOUS IMPORTANCE TO OUR SOCIETY. UNFORTUNATELY, BILLIONS OF HEALTH CARE DOLLARS ARE WASTED THROUGH FRAUD. WITH REGARD TO HEALTH CARE FRAUD, ELECTRONIC SURVEILLANCE HAS BEEN EXTREMELY IMPORTANT. IN 1993, IN NEW YORK, ELECTRONIC SURVEILLANCE OF HARDWIRED (FIXED) AND CELLULAR (MOBILE) TELEPHONES PRODUCED CRITICAL EVIDENCE IN A CASE INVOLVING WIDESPREAD MEDICARE/MEDICAID FRAUD CARRIED OUT BY NUMEROUS PHARMACIES AND PHARMACISTS. SEVENTY-NINE (79) INDIVIDUALS, INCLUDING 38 PHARMACISTS, WERE INDICTED. TO DATE, 79 INDIVIDUALS HAVE BEEN CONVICTED OR PLED GUILTY AND \$6.6 MILLION IN ASSETS ARE SUBJECT TO SEIZURE AND FORFEITURE. SIMILARLY, IN 1993, IN DETROIT, ELECTRONIC SURVEILLANCE WAS INSTRUMENTAL IN INVESTIGATING AND PROSECUTING A WIDE-SPREAD MEDICARE/MEDICAID FRAUD PERPETRATED BY NUMEROUS PHARMACIES AND PHARMACISTS. THIRTY-TWO (32) PHARMACIES/PHARMACISTS WERE PROSECUTED, AND \$4 MILLION IN CRIMINAL FORFEITURES ARE EXPECTED TO FOLLOW. THE FBI ESTIMATES THAT THE HEALTH CARE FRAUD IN EACH OF THE FOREGOING

CASES ALONE RANGED IN THE TENS OF MILLIONS OF DOLLARS.

RECENTLY, A MAJOR GOVERNMENTAL FRAUD CASE INVOLVING RUSSIAN EMIGRE ORGANIZED CRIME AND THE GAMBINO LCN ORGANIZED CRIME FAMILY WAS SUCCESSFULLY INVESTIGATED THROUGH THE USE OF AN UNDERCOVER OPERATION AND THE SUBSTANTIAL USE OF ELECTRONIC SURVEILLANCE TO INTERCEPT A NUMBER OF CELLULAR TELEPHONES. THE CRIMINAL SCHEME INVOLVED DEFRAUDING THE FEDERAL GOVERNMENT AND STATE GOVERNMENTS OF MOTOR FUEL TAXES. THE DEPARTMENT OF JUSTICE ESTIMATES THAT MORE THAN \$1 BILLION IN FEDERAL EXCISE TAX, FUNDS THAT ARE EARMARKED FOR THE HIGHWAY TRUST FUND FOR USE IN MAINTAINING THE NATION'S HIGHWAY INFRASTRUCTURE, IS ILLEGALLY "SKIMMED" EACH YEAR. AN INDICTMENT IN THE FOREGOING CASE HAS BEEN RETURNED IN NEWARK, CHARGING 14 INDIVIDUALS WITH DEFRAUDING THE FEDERAL GOVERNMENT AND THE STATE OF NEW JERSEY OUT OF MORE THAN \$60 MILLION IN TAX REVENUES AND WITH LAUNDERING \$66.2 MILLION RESULTING IN 4 CONVICTIONS TO DATE. A NUMBER OF THE SUBJECTS IN THIS INVESTIGATION UTILIZED CELLULAR TELEPHONES AND FREQUENTLY CHANGED CELLULAR TELEPHONES IN AN EFFORT TO THWART ELECTRONIC SURVEILLANCE. THE INTERCEPTED TELEPHONE CONVERSATIONS WERE CRITICAL TO PROVING THE INVOLVEMENT OF THE LCN IN THIS RUSSIAN ORGANIZED CRIME FRAUD AGAINST FEDERAL AND STATE GOVERNMENTS.

TERRORISM

A SIGNIFICANT NUMBER OF TERRORIST ACTS, INCLUDING BOMBINGS AND MURDERS, HAVE BEEN PREVENTED THROUGH THE EFFECTIVE USE OF ELECTRONIC SURVEILLANCE. MANY OF THESE TERRORIST ACTS, IF NOT PREVENTED, LIKELY WOULD HAVE HAD SUBSTANTIAL NATIONAL AND/OR INTERNATIONAL IMPLICATIONS. IN ONE CASE, THE BOMBING OF A FOREIGN CONSULATE IN THE UNITED STATES WAS PREVENTED, AND THE ELECTRONIC SURVEILLANCE EVIDENCE WAS USED IN THE SUBSEQUENT CONVICTION OF THE PRINCIPALS. IN ANOTHER CASE, A TERRORIST ROCKET ATTACK AGAINST A UNITED STATES ALLY BY A FOREIGN-BASED TERRORIST GROUP WAS THWARTED, AND THE ELECTRONIC SURVEILLANCE-BASED INVESTIGATION LED TO THE ARREST OF THE PRINCIPALS AND THE PREVENTION OF THE LOSS OF LIFE OF SCORES OF PERSONS.

IN 1986, THE EFFORTS OF THE VIOLENT EL RUKN CHICAGO STREET GANG TO SHOOT DOWN A COMMERCIAL AIRLINER WITHIN THE UNITED STATES WITH A STOLEN MILITARY WEAPON SYSTEM WAS THWARTED THROUGH ELECTRONIC SURVEILLANCE. THE FBI'S PREVENTION OF THIS ACT OF STATE-SPONSORED TERRORISM, FINANCED BY LIBYA, WHICH WOULD HAVE COST SEVERAL HUNDRED U.S. LIVES, WAS SINGULARLY ATTRIBUTABLE TO THE USE OF ELECTRONIC SURVEILLANCE -- BUT FOR THE AVAILABILITY OF THIS TECHNIQUE, ANOTHER PAN AM 103 DISASTER COULD HAVE OCCURRED ON AMERICAN SOIL.

MORE RECENTLY, IN 1993, ELECTRONIC SURVEILLANCE CONTRIBUTED TO THE INDICTMENT OF INDIVIDUALS IN THE ST. LOUIS-BASED CELL OF THE ABU NIDAL ORGANIZATION ON RICO CHARGES OF MURDER, CONSPIRACY TO COMMIT MURDER, AND CONSPIRACY TO BOMB THE ISRAELI EMBASSY IN WASHINGTON, D.C. IN 1990, FOREIGN-BASED TERRORISTS WERE PREVENTED FROM ACQUIRING A STINGER SURFACE-TO-AIR MISSILE WHICH WAS TO BE EMPLOYED IN A TERRORIST ACT WHEREIN NUMEROUS PEOPLE WOULD UNDOUBTEDLY HAVE BEEN KILLED. ALSO, IN 1989, AS A DIRECT RESULT OF COURT-ORDERED ELECTRONIC SURVEILLANCE IN A TERRORIST-RELATED MATTER, INFORMATION WAS OBTAINED WHICH RESULTED IN THE CONVICTION OF TWO INDIVIDUALS FOR THE BRUTAL HOMICIDE OF THEIR 16-YEAR OLD DAUGHTER.

BEYOND THE FOREGOING INSTANCES, OVER THE LAST DECADE NUMEROUS OTHER TERRORIST-RELATED INVESTIGATIONS HAVE UTILIZED ELECTRONIC SURVEILLANCE TO: PREVENT A ROCKET ATTACK AGAINST AN FBI FIELD OFFICE; PREVENT AN ATTACK ON A NUCLEAR POWER FACILITY; SOLVE SEVERAL MURDERS; IDENTIFY THE PERPETRATORS OF A \$7,000,000 ARMED ROBBERY; AND SOLVE AND PREVENT SEVERAL BOMBINGS BY ANTI-CASTRO GROUPS IN MIAMI, FLORIDA.

VIOLENT CRIME

MANY VIOLENT CRIMES, INCLUDING MURDER, HAVE BEEN SOLVED AND A SIGNIFICANT NUMBER PREVENTED BY LAW ENFORCEMENT'S "REAL TIME" RESPONSE TO, AND PREVENTIVE ACTIONS TAKEN AS A RESULT OF CONVERSATIONS INTERCEPTED THROUGH ELECTRONIC SURVEILLANCE.

ELECTRONIC SURVEILLANCE HAS BEEN USED IN COMBATTING AND SOLVING VIOLENT CRIMES PERPETRATED BY BOTH ORGANIZED CRIMINAL GROUPS AND BY INDIVIDUALS. THE FOLLOWING ARE RECENT EXAMPLES OF CASES IN WHICH ELECTRONIC SURVEILLANCE HAS BEEN CRUCIAL IN SAVING LIVES OR PREVENTING VIOLENT ACTS FROM OCCURRING:

- O CONVERSATIONS OF MEMBERS OF THE NEW ENGLAND LCN FAMILY WERE INTERCEPTED WHEREIN THE MURDERS OF THREE INDIVIDUALS WERE PLANNED, AND DETAILS CONCERNING SIX PRIOR MURDERS WERE DISCUSSED. OF THE THREE PLANNED MURDERS, TWO WERE PREVENTED BY THE FBI; THE THIRD COULD NOT BE PREVENTED BECAUSE OF AN INABILITY TO LOCATE THE VICTIM PRIOR TO HIS MURDER.
- O ONE OF THE MOST VIOLENT ASIAN ORGANIZED CRIME GANGS ACTIVE IN THE NEW YORK CITY AREA IS THE GREEN DRAGONS, WHICH, AS OF 1990, WAS DIRECTED TELEPHONICALLY BY KIN FEI WONG FROM THE PEOPLE'S REPUBLIC OF CHINA. THE GREEN DRAGONS GANG PERPETRATED MURDER, ARMED ROBBERIES, HOME INVASIONS, EXTORTION, DRUG TRAFFICKING, AND WERE INVOLVED IN THE OBSTRUCTION OF JUSTICE. COURT-ORDERED ELECTRONIC SURVEILLANCE PROVIDED EVIDENCE OF THESE CRIMES AND ALSO DISCLOSED THAT THE GREEN DRAGONS WERE ABOUT TO ENGAGE IN A "SHOOT OUT" WITH A RIVAL ASIAN GANG. IMMEDIATELY ACTING UPON THIS INFORMATION, 16 MEMBERS OF THE GROUP WERE ARRESTED BY FBI AGENTS AND POLICE OFFICERS AND AN IMMINENT VIOLENT CONFRONTATION AND LOSS OF LIFE WERE PREVENTED. BASED PARTLY UPON EVIDENCE DERIVED FROM ELECTRONIC SURVEILLANCE, ALL DEFENDANTS WERE FOUND GUILTY OF RACKETEERING, RACKETEERING CONSPIRACY, AND NUMEROUS SUBSTANTIVE COUNTS WHICH INCLUDED MURDER, KIDNAPPING, HOME INVASIONS, ARMED ROBBERY, EXTORTION AND BRIBERY OF A PUBLIC OFFICIAL.
- O IN 1991, THE MURDER OF A UNITED STATES COURT OF APPEALS JUDGE WAS SOLVED AND A CONVICTION OBTAINED BASED IN PART UPON ELECTRONIC SURVEILLANCE INFORMATION.

- O IN A NOTABLE 1990 "SEXUAL EXPLOITATION" OF CHILDREN CASE WHICH RELIED HEAVILY UPON ELECTRONIC SURVEILLANCE, THE FBI THWARTED TWO INDIVIDUALS WHO WERE CONSPIRING TO ABDUCT, TORTURE, AND KILL A TEENAGE BOY FOR THE PURPOSE OF MAKING A "SNUFF MURDER" FILM.
- O IN 1993, IN GREENE COUNTY, OHIO, A 10-YEAR OLD TRIPLE HOMICIDE WAS FINALLY SOLVED, AND EVIDENCE CRITICAL FOR SUCCESSFUL PROSECUTION WAS OBTAINED THROUGH THE USE OF ELECTRONIC SURVEILLANCE. THE VICTIMS, TWO MEN AND A PREGNANT WOMAN, HAD BEEN SHOT EXECUTION-STYLE, AND SUBSEQUENTLY THEIR THROATS HAD BEEN SLIT AND THEIR SKULLS HAD BEEN CRUSHED BY THE MURDERERS.

FOREIGN COUNTERINTELLIGENCE (FCI)

BECAUSE ANY DISCUSSION OF THE IMPORTANCE OF FISA-BASED ELECTRONIC SURVEILLANCE WOULD INVOLVE HIGHLY SENSITIVE MATTERS AND HIGHLY CLASSIFIED INFORMATION, SUFFICE IT TO SAY THAT INFORMATION DERIVED FROM FISA ELECTRONIC SURVEILLANCE IS CRITICAL TO THE PRESIDENT OF THE UNITED STATES, THE NATIONAL SECURITY COUNCIL, THE INTELLIGENCE COMMUNITY, THE DEPARTMENT OF DEFENSE, AND THE STATE DEPARTMENT. SUCH INFORMATION IS OF GREAT IMPORTANCE AS OUR NATION'S LEADERS ESTABLISH POLICY AND SAFEGUARD THE NATION'S DEFENSE AND NATIONAL SECURITY.

CONSEQUENCES OF THE LOSS OF ELECTRONIC SURVEILLANCE

AS INDICATED ABOVE, SOCIETY'S MOST DANGEROUS CRIMINAL ORGANIZATIONS AND GROUPS RELY HEAVILY UPON THE USE OF TELECOMMUNICATIONS. ADDITIONALLY, SUCH ORGANIZATIONS TEND TO TAKE ADVANTAGE OF ADVANCED TELECOMMUNICATIONS AND SERVICES TO CONDUCT AND CARRY OUT THEIR ILLEGAL ACTIVITIES. EVIDENCE IS DEVELOPING THAT INDICATES CRIMINAL ORGANIZATIONS ARE ALSO INCREASINGLY LOOKING FOR WAYS TO AVOID LAW ENFORCEMENT'S ELECTRONIC SURVEILLANCE BY FREQUENTLY CHANGING THEIR . TELECOMMUNICATIONS DEVICES AND TELEPHONE NUMBERS, MODIFYING AND REPROGRAMMING THEIR CELLULAR TELEPHONE IDENTIFICATION NUMBERS AND

CODES, AND UTILIZING CALL-FORWARDING FEATURES, ETC. INCREASED USE OF CELLULAR TELEPHONES, CALL-FORWARDING FEATURES, AND EVASIVE EFFORTS HAVE ALREADY HAD A NEGATIVE IMPACT UPON ELECTRONIC SURVEILLANCE AND LAW ENFORCEMENT'S ABILITY TO PROTECT THE PUBLIC AND EFFECTIVELY ENFORCE THE LAW. THE FOREGOING CASES DIRECTLY DEMONSTRATE THE PUBLIC SAFETY AND LAW ENFORCEMENT BENEFITS **DIRECTLY ATTRIBUTABLE TO THE USE OF ELECTRONIC SURVEILLANCE.** THEY ALSO INDICATE THE KIND OF NEGATIVE IMPACTS AND SOCIETAL HARMS THAT WOULD RESULT IF THERE WERE A LOSS OR DIMINISHMENT OF THE ELECTRONIC SURVEILLANCE TECHNIQUE. INDEED, LOSS OF A VIABLE, EFFECTIVE ELECTRONIC SURVEILLANCE TECHNIQUE WOULD RESULT IN:

- A SUBSTANTIAL LOSS OF LIFE, ATTRIBUTABLE TO THE INABILITY OF LAW ENFORCEMENT TO PREVENT PLANNED TERRORIST ACTS AND MURDERS.
- A SUBSTANTIAL INCREASE IN ECONOMIC HARM (IN THE BILLIONS OF DOLLARS) TO BUSINESS, INDUSTRY, LABOR UNIONS, AND SOCIETY GENERALLY CAUSED BY THE GROWTH/EMERGENCE OF ORGANIZED CRIME GROUPS AND ACTIVITIES;
- A SUBSTANTIAL INCREASE IN THE CORRUPTION OF LEGITIMATE BUSINESS, INDUSTRY, AND LABOR UNIONS CAUSED BY THE GROWTH/EMERGENCE OF ORGANIZED CRIME GROUPS;
- A SUBSTANTIAL INCREASE IN THE AVAILABILITY AND REDUCED COST OF NARCOTICS AND ILLEGAL DRUGS, AS WELL AS THE ATTENDANT PERSONAL, SOCIETAL, AND ECONOMIC HARM (NUMEROUS DEATHS, RAVAGED LIVES, AND INCREASED ECONOMIC HARM IN THE BILLIONS OF DOLLARS);
- A SUBSTANTIAL INCREASE IN UNDETECTED AND UNPROSECUTED PUBLIC CORRUPTION AND FRAUD AGAINST THE GOVERNMENT (IN THE BILLIONS OF DOLLARS) AND A RESULTING LOST TRUST IN GOVERNMENT;
- A SUBSTANTIAL INCREASE IN UNDETECTED AND UNPROSECUTED TERRORIST BOMBINGS, MURDERS, AND OTHER ACTS WITH THE ATTENDANT LOSS OF NUMEROUS LIVES AND BILLIONS OF DOLLARS IN ECONOMIC HARM;

- O A SUBSTANTIAL INCREASE IN UNPROSECUTED CRIMINAL CASES OF ALL KINDS AND THE POTENTIAL FOR A SUBSTANTIAL INCREASE IN ACQUITTALS AND HUNG JURIES OCCASIONED BY THE LACK OF DIRECT AND PERSUASIVE ELECTRONIC SURVEILLANCE EVIDENCE.

ELECTRONIC SURVEILLANCE: SURGICAL USE WITHOUT ABUSE

IN PASSING THE TITLE III LEGISLATION, CODIFIED AT 18 U.S.C. 2510-21, CONGRESS ENACTED A COMPREHENSIVE ELECTRONIC SURVEILLANCE REGIMEN THAT CAREFULLY BALANCED THE COMMUNICATIONS SECURITY NEEDS AND PRIVACY RIGHTS OF INDIVIDUALS WITH THE LEGITIMATE NEEDS OF LAW ENFORCEMENT TO PROTECT THE PUBLIC AND EFFECTIVELY ENFORCE THE LAW. ABOVE AND BEYOND THE TRADITIONAL REQUIREMENTS OF THE FOURTH AMENDMENT COMPLIANCE (SUCH AS PROBABLE CAUSE, THE NEED FOR IMPARTIAL JUDICIAL REVIEW AND A WARRANT, PARTICULARITY AS TO THE OBJECT OF THE SEARCH, PROMPT EXECUTION OF THE ELECTRONIC SEARCH, ETC.), CONGRESS ALSO SPECIFIED THAT ELECTRONIC SURVEILLANCE COULD BE USED, GENERALLY SPEAKING, ONLY AS A LAST RESORT (WHEN OTHER INVESTIGATIVE TECHNIQUES FAILED OR WERE TOO DANGEROUS); ONLY FOR SERIOUS FELONY OFFENSES; AND ONLY FOR SPECIFIC CRIMINAL COMMUNICATIONS. THE ACQUISITION OF NON-CRIMINAL, NON-RELEVANT COMMUNICATIONS IS FORBIDDEN AND SUCH COMMUNICATIONS MUST BE CAREFULLY MINIMIZED.

CONGRESS HAS ALSO ENACTED AN ELECTRONIC SURVEILLANCE REGIMEN FOR USE IN INTELLIGENCE BASED INVESTIGATIONS, THE FOREIGN INTELLIGENCE SURVEILLANCE ACT OF 1978 (FISA), CODIFIED AT 50 U.S.C. 1801-1811. CONTRARY TO THE ASSERTIONS OF SOME, ELECTRONIC SURVEILLANCE CONDUCTED PURSUANT TO TITLE III OR FISA MAY NOT BE (AND ARE NOT) EMPLOYED AGAINST INDIVIDUALS EXERCISING THEIR FIRST AMENDMENT RIGHTS, SUCH AS BY ENGAGING IN UNPOPULAR, POLITICAL, OR ANTI-GOVERNMENTAL DISCOURSE.

AN OBJECTIVE REVIEW AND ASSESSMENT OF THE TITLE III AND FISA STATUTES, AND OF THE CONDUCT OF ELECTRONIC SURVEILLANCE BY LAW ENFORCEMENT PURSUANT TO THESE STATUTES, INDICATE THAT ELECTRONIC SURVEILLANCE HAS BEEN CONDUCTED SPARINGLY,

JUDICIOUSLY, AND IN COMPLIANCE WITH THE LETTER OF THE LAW AND THE SPIRIT OF CONGRESS' INTENT. AS DEMONSTRATED BY THE LIVES SAVED AND IMPORTANT INVESTIGATIONS AND PROSECUTIONS SUCCESSFULLY COMPLETED, THE TITLE III STATUTORY REGIMEN HAS SERVED BOTH SOCIETY AND LAW ENFORCEMENT EXTREMELY WELL. MOREOVER, AFTER 25 YEARS OF USAGE, THERE IS NO EVIDENCE OF SIGNIFICANT ABUSE. STATISTICS COMPILED BY THE FBI, WHICH IS CHARGED WITH INVESTIGATING VIOLATIONS OF THE FEDERAL "WIRETAP" STATUTE BASED UPON ACTS OF ILLEGAL ELECTRONIC SURVEILLANCE AND WIRETAPPING, INDICATE THAT INSTANCES OF ILLEGAL WIRETAPPING ARE VERY, VERY RARE.

ELECTRONIC SURVEILLANCE TECHNICAL ASSISTANCE

WHEN THE TITLE III LEGISLATION WAS ENACTED BY CONGRESS IN 1968, THERE WAS NO SPECIFIC PROVISION FOR TECHNICAL OR OTHER ASSISTANCE TO LAW ENFORCEMENT. WITH REGARD TO WIRE COMMUNICATIONS, LAW ENFORCEMENT NECESSARILY RELIES UPON THE TELECOMMUNICATION SERVICE PROVIDER'S ASSISTANCE IN IDENTIFYING THE TARGET'S WIRE PAIRS AND THEIR LINE "APPEARANCES," AND UPON THE SERVICE PROVIDER'S FURNISHING OF LEASED LINES TO ENABLE THE INTERCEPTED COMMUNICATIONS TO BE TRANSMITTED TO A SECURE, LAW ENFORCEMENT MONITORING FACILITY.

ALTHOUGH THE SERVICE PROVIDER ASSISTANCE REQUIREMENT WAS THOUGHT TO BE SELF-EVIDENT AND IMPLICIT IN THE TITLE III LEGISLATION, CERTAIN SERVICE PROVIDERS INITIALLY RESISTED PROVIDING LAW ENFORCEMENT WITH NEEDED ASSISTANCE, EVEN WHEN DIRECTED TO DO SO BY COURT ORDER. SEE, E.G., APPLICATION OF UNITED STATES, 427 F.2D 639 (9TH CIR. 1970). AS A RESULT, CONGRESS WAS COMPELLED TO AMEND THE TITLE III STATUTE IN 1970 AND EXPRESSLY FIX THE ASSISTANCE RESPONSIBILITY THEREIN. THE ASSISTANCE PROVISION, AS AMENDED, AND CODIFIED AT 18 U.S.C 2518(4), STATES:

"AN ORDER AUTHORIZING THE INTERCEPTION OF A WIRE, ORAL, OR ELECTRONIC COMMUNICATION UNDER THIS CHAPTER SHALL, UPON REQUEST OF THE APPLICANT, DIRECT THAT A PROVIDER OF WIRE OR ELECTRONIC COMMUNICATION SERVICE, LANDLORD, CUSTODIAN OR OTHER PERSON SHALL FURNISH THE APPLICANT

FORTHWITH ALL INFORMATION, FACILITIES, AND TECHNICAL ASSISTANCE NECESSARY TO ACCOMPLISH THE INTERCEPTION UNOBTUSIVELY AND WITH A MINIMUM OF INTERFERENCE WITH THE SERVICES THAT SUCH SERVICE PROVIDER, LANDLORD, CUSTODIAN, OR PERSON IS ACCORDING THE PERSON WHOSE COMMUNICATIONS ARE TO BE INTERCEPTED. ANY PROVIDER OF WIRE OR ELECTRONIC COMMUNICATION SERVICE, LANDLORD, CUSTODIAN OR OTHER PERSON FURNISHING SUCH FACILITIES OR TECHNICAL ASSISTANCE SHALL BE COMPENSATED THEREFORE BY THE APPLICANT FOR REASONABLE EXPENSES INCURRED IN PROVIDING SUCH FACILITIES OR ASSISTANCE." (EMPHASIS ADDED)

THE FISA STATUTE, ENACTED IN 1978, CONTAINS A SIMILAR ASSISTANCE PROVISION, CODIFIED AT 50 U.S.C 1805 (B)(2). SO ALSO DO THE PEN REGISTER AND TRAP AND TRACE STATUTES. SEE 18 U.S.C. 3124(a)(b).

IT IS VERY IMPORTANT TO UNDERSTAND THAT TELEPHONE COMPANIES HISTORICALLY HAVE BEEN EXTREMELY CONSERVATIVE, AND OFTEN HAVE DECLINED TO PROVIDE LAW ENFORCEMENT WITH NECESSARY TECHNICAL ASSISTANCE, EVEN WHEN SERVED WITH COURT ORDERS. FOR EXAMPLE, SOME TELEPHONE COMPANIES INITIALLY RESISTED PROVIDING LAW ENFORCEMENT WITH EVEN MINOR "LEASED LINE" ASSISTANCE TO ALLOW LAW ENFORCEMENT TO CARRY OUT A PEN REGISTER INVESTIGATION, ALTHOUGH SERVED WITH A FEDERAL SEARCH WARRANT. THIS RESISTANCE TO PEN REGISTER ASSISTANCE WAS REMOVED BY THE SUPREME COURT IN UNITED STATES V. NEW YORK TELEPHONE CO., 434 U.S. 159 (1977). SOME TELEPHONE COMPANIES ALSO RESISTED PROVIDING RELATIVELY MINOR ASSISTANCE TO EFFECT A TRAP AND TRACE OF DIALED NUMBER INFORMATION WHEN SERVED WITH A FEDERAL COURT ORDER. FEDERAL COURT OF APPEALS ACTION WAS REQUIRED TO OBTAIN SUCH TRAP AND TRACE ASSISTANCE TO TRACE DIALED NUMBER INFORMATION. UNITED STATES V. MOUNTAIN STATES TELEPHONE AND TELEGRAPH COMPANY, 616 F.2D 1122 (9TH CIR. 1980); IN RE APPLICATION OF UNITED STATES, 610 F.2D 1148 (3RD CIR. 1979); MICHIGAN BELL TELEPHONE COMPANY V. UNITED STATES, 565 F.2D 385 (6TH CIR. 1977). THE LESSON FROM

SUCH INCIDENTS IS CLEAR: SOME TELECOMMUNICATIONS COMPANIES, INCLUDING COMMON CARRIERS, WHO ARE CONCERNED WITH THEIR LEGAL LIABILITIES WILL ACT ONLY WHEN THE LAW IS CLEAR AS TO THEIR RESPONSIBILITIES AND WHEN PRESENTED WITH A COURT ORDER.

IN THE AREAS OF PEN REGISTERS AND TRAP AND TRACE DEVICES, COURTS HAVE REQUIRED TELECOMMUNICATION SERVICE PROVIDERS TO EXTEND TECHNICAL AND PHYSICAL ASSISTANCE TO LAW ENFORCEMENT, IN ORDER TO EFFECTUATE COURT ORDERS. THERE ARE, HOWEVER, NO FEDERAL CASES CONSTRUING THE TITLE III OR FISA STATUTORY "ASSISTANCE" PROVISIONS. ATTORNEYS WHO HAVE ANALYZED THESE ASSISTANCE PROVISIONS BELIEVE THAT THEIR CURRENT LANGUAGE DOES NOT CLEARLY MANDATE THAT SERVICE PROVIDERS AFFIRMATIVE MUST TAKE ANY STEPS OR DEVELOP ANY TECHNICAL SOLUTIONS TO ACCOMMODATE OR EFFECTUATE A COURT'S ELECTRONIC SURVEILLANCE ORDER. THUS, THE ISSUE AS TO THE NATURE AND EXTENT OF SERVICE PROVIDER ASSISTANCE REMAINS AN OPEN, AND OFTEN HOTLY DEBATED, QUESTION.

THE QUESTION HAS BEEN RAISED BY SOME IF REQUESTING OR REQUIRING GREATER ELECTRONIC SURVEILLANCE TECHNICAL ASSISTANCE OF SERVICE PROVIDERS TO CARRY OUT A COURT ORDER THROUGH EITHER HARDWARE- OR SOFTWARE-BASED MODIFICATIONS OR DEVELOPMENTS EXTENDS LAW ENFORCEMENT'S AUTHORITY. THERE APPEARS TO BE GENERAL AGREEMENT WITHIN THE GOVERNMENT AND INDUSTRY THAT THIS WOULD NOT EXTEND LAW ENFORCEMENT'S ELECTRONIC SURVEILLANCE AUTHORITY. THIS AGREEMENT EXTENDS TO LAW ENFORCEMENT'S LEGAL AUTHORITY OR ENTITLEMENT TO OBTAIN THE CONTENT OF A CRIMINAL TARGET'S COMMUNICATIONS OR DIALED NUMBER INFORMATION TRANSMITTED VIA A TELECOMMUNICATIONS NETWORK.

SOME HAVE STATED THAT REQUIRING TELECOMMUNICATION SERVICE PROVIDERS TO EXPEND ADDITIONAL TECHNICAL OR MONETARY RESOURCES, EVEN PURSUANT TO COURT ORDER, TO HELP LAW ENFORCEMENT EFFECT ELECTRONIC SURVEILLANCE IS UNWARRANTED OR UNPRECEDENTED. HOWEVER, HISTORICALLY TELECOMMUNICATION SERVICE PROVIDERS HAVE BEEN REQUIRED TO ALTER THEIR OPERATIONS AND ACTIVITIES TO MEET LAW ENFORCEMENT REQUIREMENTS. FOR EXAMPLE, SERVICE PROVIDERS HAVE BEEN REQUIRED BY REGULATION TO MAINTAIN TELEPHONE TOLL

RECORDS LONGER THAN OPERATIONALLY NECESSARY, AND GENERALLY THEY DEDICATE TIME, HUMAN RESOURCES, AND HENCE MONEY, TO PROVIDE LAW ENFORCEMENT AGENCIES WITH SUCH SUBSCRIBER INFORMATION. FURTHER, BY WAY OF PRECEDENT, CONGRESS HAS ENACTED PUBLIC SAFETY/PUBLIC WELFARE LEGISLATION CONCERNING TELECOMMUNICATION SERVICE PROVIDERS IN THE AREA OF INTEROPERABLE EQUIPMENT TO ASSIST THE HEARING-IMPAIRED AND IN THE AREA OF TELEPHONICALLY TRANSMITTED PORNOGRAPHIC COMMUNICATIONS (SO CALLED "DIAL-A-PORN"). ALSO, MANY LOCALITIES REQUIRE BY LAW THAT THE TELECOMMUNICATION LOCAL EXCHANGE CARRIERS PROVIDE "911" EMERGENCY SERVICE, THE COST OF WHICH IS PASSED ON TO ALL SUBSCRIBERS.

WITHIN THE UNITED STATES, THERE ARE NUMEROUS OTHER PUBLIC SAFETY/PUBLIC WELFARE LAWS AND REGULATIONS WHICH AFFECT A NUMBER OF INDUSTRIES AND BUSINESSES AND MANDATE TECHNICAL EFFORTS AND MONETARY EXPENSES (E.G., REQUIRED SPRINKLER SYSTEMS, SMOKE DETECTORS, FIRE ALARMS, FIRE ESCAPES, ETC., IN OFFICES, FACTORIES, APARTMENT COMPLEXES, ETC.; SAFETY BELTS, "AIR BAGS," CATALYTIC CONVERTERS, AND EMISSION CONTROL DEVICES IN VEHICLES). ON BALANCE, WHEN LAW ENFORCEMENT'S COURT-ORDERED USE OF ELECTRONIC SURVEILLANCE IS VIEWED IN TERMS OF ITS IMPORTANT, AND EVEN CRITICAL, UTILITY IN PREVENTING AND SOLVING CRIMES, AND AS A PUBLIC SAFETY REQUIREMENT, THERE CAN BE NO SERIOUS DOUBT THAT A POLICY DECISION REQUIRING SUCH TECHNICAL ASSISTANCE BY LAW IS CONSISTENT WITH PAST SOCIETAL AND GOVERNMENTAL PRACTICES.

SUMMARY OF TECHNOLOGICAL IMPEDIMENTS

PRIOR TO 1984, THE MAJORITY OF LOCAL AND LONG DISTANCE TELECOMMUNICATIONS WERE CARRIED BY AT&T, WHICH HELD A VIRTUAL MONOPOLY ON THESE SERVICES. THIS RESULTED IN AN HOMOGENEOUS NETWORK IN WHICH THE TECHNOLOGIES USED TO CONDUCT BUSINESS WERE THE SAME THROUGHOUT THE NETWORK. ADDITIONALLY, BECAUSE OF AN ABSENCE OF COMPETITION, NEW TECHNOLOGIES WERE INTRODUCED SLOWLY AND BY ONLY A SMALL NUMBER OF MANUFACTURERS.

SINCE THE DIVESTITURE OF AT&T IN 1984, THE NUMBER OF

SERVICE PROVIDERS, AS WELL AS THE DIVERSITY OF TECHNOLOGIES, HAS GROWN RAPIDLY AND DRAMATICALLY. FOR EXAMPLE, THE NUMBER OF CARRIERS PROVIDING LOCAL TELEPHONE SERVICE IS NOW OVER 1,400. A SEPTEMBER 1992 DECISION BY THE FEDERAL COMMUNICATIONS COMMISSION IS FACILITATING EVEN GREATER COMPETITION IN THIS AREA. AS A RESULT, THE INDUSTRY WILL BEGIN TO SEE NEW PROVIDERS OF SERVICE AND ALREADY HAS BEGUN TO SEE NEW BUSINESS PARTNERSHIPS AMONG EXISTING SERVICE PROVIDERS. ALSO, THE NUMBER OF LONG DISTANCE CARRIERS HAS GROWN FROM ESSENTIALLY ONE IN 1984 TO OVER 300 TODAY. WITH THE ADVENT OF WIRELESS TECHNOLOGIES, SUCH AS CELLULAR, THE NUMBER OF SERVICE PROVIDERS GREW AGAIN. TODAY, THERE ARE OVER 160 CELLULAR SERVICE PROVIDERS. THE INTRODUCTION OF NEW TECHNOLOGIES, AS WELL AS ACTIONS TAKEN BY THE FEDERAL COURTS AND THE FEDERAL COMMUNICATIONS COMMISSION, HAVE RESULTED IN GREATER NUMBERS AND MORE DIVERSITY AMONG SERVICE PROVIDERS. AS A RESULT, LAW ENFORCEMENT AGENCIES HAVE HAD TO WORK WITH MANY DIFFERENT SERVICE PROVIDERS TO OBTAIN THE ASSISTANCE NECESSARY TO CONDUCT WIRETAPS. NUMEROUS SITUATIONS HAVE ARISEN WHERE SERVICE PROVIDERS WHO WERE INEXPERIENCED WITH COURT AUTHORIZED WIRETAPS HAVE BEEN UNABLE TO PROVIDE ASSISTANCE TO LAW ENFORCEMENT AGENCIES BECAUSE OF A LACK OF UNDERSTANDING OF THE LEGITIMATE REQUIREMENTS OF LAW ENFORCEMENT.

TRADITIONALLY, COMMON CARRIERS HAVE OFFERED ESSENTIALLY "FIXED POINT" TELECOMMUNICATIONS: THAT IS TO SAY, COMMUNICATIONS GENERATED BY, OR INTENDED FOR, A CUSTOMER AND TRANSMITTED TO A FIXED LOCATION CORRESPONDING TO A SPECIFIC TELEPHONE NUMBER. HISTORICALLY, THESE COMMUNICATIONS HAVE BEEN TRANSMITTED OVER COMMON CARRIER FACILITIES, SUCH AS TELEPHONE WIRES THAT WERE DEDICATED TO A CUSTOMER'S SPECIFIC TELEPHONE NUMBER (OFTEN REFERRED TO AS A SUBSCRIBER'S "LOOP"). IN THE PAST, WHEN LAW ENFORCEMENT AGENCIES CONDUCTED COURT-AUTHORIZED ELECTRONIC SURVEILLANCE OR "WIRETAPS" ON A SUBJECT'S TRADITIONAL "LOCAL LOOP," THEY WERE VIRTUALLY ASSURED OF INTERCEPTING THE CONTENT OF ALL COMMUNICATIONS (AS WELL AS THE RELATED DIALING INFORMATION)

ASSOCIATED WITH THE SUBJECT'S TELEPHONE NUMBER SET FORTH IN THE COURT ORDER.

OVER RECENT YEARS, ADVANCES IN TELECOMMUNICATIONS TECHNOLOGIES, AS WELL AS THE INCREASING NUMBER OF COMMON CARRIERS (APPROXIMATELY 2,000) ENTERING THE TELECOMMUNICATIONS MARKETPLACE, HAVE INTRODUCED NEW SOPHISTICATED SERVICES AND FEATURES THAT ALLOW FOR THE EFFICIENT TRANSMISSION OF MULTIPLE, SIMULTANEOUS COMMUNICATIONS OF MULTIPLE SUBSCRIBERS. SUCH COMMUNICATIONS ARE TRANSMITTED OVER FIBER OPTIC LINES AND WIRE FACILITIES THAT PREVIOUSLY WERE DEDICATED TO A SINGLE COMMUNICATION AND A SINGLE SUBSCRIBER. OTHER ADVANCED COMMUNICATIONS SERVICES (SUCH AS CELLULAR TELEPHONES) AND FEATURES (SUCH AS CALL FORWARDING WHICH PERMITS CUSTOMERS TO REDIRECT CALLS INTENDED FOR THEM) UNDERMINE THE NECESSITY FOR COMMUNICATIONS TO BE TRANSMITTED ALWAYS TO THE SAME SPECIFIC LOCATION OR THROUGH THE SAME WIRELINE LOOP. LIKEWISE, "FOLLOW-ME" FEATURES AND SERVICES EXPAND THE NOTION OF CALL FORWARDING TO NATIONAL PROPORTIONS. FURTHER, COMMON CARRIERS' DEPLOYMENT OF THE PERSONAL COMMUNICATIONS SERVICES (PCS) IN THE NEAR FUTURE WILL ENABLE USERS TO DEFINE THEIR OWN SET OF SUBSCRIBED SERVICES, USE ANY FIXED OR MOBILE TERMINAL OR TELEPHONE INSTRUMENT, AND INITIATE AND RECEIVE CALLS ACROSS MULTIPLE NETWORKS WITHOUT REGARD TO THEIR GEOGRAPHIC LOCATION. ALL OF THESE "FOLLOW-ME-TYPE" SERVICES, IN EFFECT, DISASSOCIATE A SUBSCRIBER'S NUMBER FROM A FIXED LOCAL LOOP. THUS, LAW ENFORCEMENT'S ABILITY TO CONDUCT SUCCESSFULLY COURT-ORDERED ELECTRONIC SURVEILLANCE IS GREATLY HAMPERED.

AS A RESULT OF THESE AND OTHER NEW AND ADVANCED TECHNOLOGIES, COMMON CARRIERS ARE NO LONGER ABLE TO ENSURE THEIR ABILITY TO ISOLATE SPECIFIC COMMUNICATIONS (AND DIALING INFORMATION) ASSOCIATED WITH THE SUBJECTS OF COURT-ORDERED SURVEILLANCE, TO THE EXCLUSION OF ALL OTHER SUBSCRIBERS' COMMUNICATIONS AND DIALING INFORMATION. INDUSTRY REPRESENTATIVES HAVE BLUNTLY TOLD LAW ENFORCEMENT THAT THE EXISTING

TELECOMMUNICATIONS SYSTEMS AND NETWORKS WILL THWART COURT AUTHORIZED INTERCEPTS. THE ABOVE-DESCRIBED SERVICES AND FEATURES AND THE NEW TELECOMMUNICATION SYSTEMS PLANNED FOR FUTURE IMPLEMENTATION, BOTH IN THEIR CURRENT AND PLANNED CONFIGURATIONS, OFTEN PREVENT, AND WILL CONTINUE TO PREVENT COMMON CARRIERS FROM PROVIDING LAW ENFORCEMENT WITH ACCESS TO ALL OF THE COMMUNICATIONS AND DIALING INFORMATION THAT ARE THE SUBJECT OF ELECTRONIC SURVEILLANCE AND PEN REGISTER COURT ORDERS.

THE ATTACHED CHARTS (PAST OPERATING ENVIRONMENT, PRESENT OPERATING ENVIRONMENT, AND FUTURE OPERATING ENVIRONMENT) DEPICT THE INCREASINGLY COMPLEX TELECOMMUNICATIONS ENVIRONMENT IN WHICH LAW ENFORCEMENT HAS OPERATED AND WILL CONTINUE TO OPERATE WHEN ATTEMPTING TO EXECUTE COURT-AUTHORIZED ELECTRONIC SURVEILLANCES.

OVER THE LAST DECADE, IT IS CONSERVATIVELY ESTIMATED THAT SEVERAL HUNDRED ELECTRONIC SURVEILLANCE AND PEN REGISTER AND TRAP AND TRACE COURT ORDERS HAVE BEEN FRUSTRATED, IN WHOLE OR IN PART, BY VARIOUS TECHNOLOGICAL IMPEDIMENTS. DURING 1993, THE FBI, THROUGH AN INFORMAL SURVEY OF FEDERAL, STATE, AND LOCAL LAW ENFORCEMENT, COLLECTED INFORMATION REGARDING THE EXECUTION OF RECENT ELECTRONIC SURVEILLANCE COURT ORDERS (INCLUDING AUTHORIZATIONS FOR CALL CONTENT, PEN REGISTER, AND TRAP AND TRACE) IN ORDER TO GAUGE HOW MANY COURT ORDERS HAVE BEEN FRUSTRATED OR DELAYED DUE TO TECHNOLOGY-BASED PROBLEMS. THE SURVEY REVEALED 91 INSTANCES IN WHICH LAW ENFORCEMENT AGENCIES PARTICIPATING IN THE SURVEY WERE PRECLUDED FROM IMPLEMENTING OR FULLY IMPLEMENTING COURT ORDERS FOR ELECTRONIC SURVEILLANCE DUE TO VARIOUS TECHNOLOGICAL IMPEDIMENTS. THE MAJORITY OF THE PROBLEMS WERE ENCOUNTERED DURING ATTEMPTS TO EXECUTE ORDERS REGARDING ELECTRONIC SURVEILLANCE ACTIVITIES RELATING TO CELLULAR TELEPHONE SYSTEMS (33%) AND "FIXED" OR WIRELINE COMMUNICATIONS THAT EMPLOYED CUSTOM CALLING FEATURES (32%). WITH RESPECT TO CELLULAR SYSTEMS, PROBLEMS HAVE RANGED FROM A TECHNICAL INABILITY ON THE PART OF THE CELLULAR COMMON CARRIER TO ASSIST LAW ENFORCEMENT, TO CELLULAR SYSTEMS THAT WERE NOT CAPABLE OF

ISOLATING AND COLLECTING COMMUNICATIONS AND/OR PEN REGISTER INFORMATION (DIALED NUMBERS) ASSOCIATED WITH SUBJECT'S TELEPHONE COMMUNICATIONS. A SEPARATE CATEGORY OF TECHNICAL PROBLEMS ASSOCIATED WITH CELLULAR SYSTEMS RELATES TO THE INABILITY OF SOME CELLULAR CARRIERS TO COMPLY WITH COURT ORDERS DUE TO A LIMITED CAPACITY ASSOCIATED WITH THE CARRIER'S PARTICULAR SYSTEM (11%). THE FOLLOWING ARE EXAMPLES TO ILLUSTRATE SOME OF THE IMPEDIMENTS ENCOUNTERED:

1. A FEDERAL INVESTIGATION OF A MAJOR NARCOTICS ORGANIZATION OPERATING IN THE NORTHEASTERN UNITED STATES WAS HAMPERED WHEN THE CELLULAR TELEPHONE SERVICE PROVIDER WAS UNABLE TO FULFILL REQUESTS FOR COURT-ORDERED WIRETAPS DUE TO THE PROVIDER'S TECHNICAL LIMITATIONS.
2. AN ORGANIZED CRIME AND DRUG TRAFFICKING TASK FORCE INVESTIGATION IN THE SOUTHEASTERN U. S. WAS UNABLE TO CONDUCT A COURT-ORDERED WIRETAP AS THE CELLULAR TELEPHONE SERVICE PROVIDER WAS UNABLE TO PROVIDE LAW ENFORCEMENT WITH ACCESS TO THE SUBJECT'S LONG DISTANCE COMMUNICATIONS MADE THROUGH THE PROVIDERS CELLULAR SERVICE.
3. TWO DIFFERENT CELLULAR SERVICE PROVIDERS IN THE MID-WESTERN U.S. WERE UNABLE TO COMPLY WITH SEPARATE FEDERAL COURT-ORDERS REQUESTING PEN REGISTER OR DIALED NUMBER INFORMATION FROM A SUSPECTED DRUG TRAFFICKER'S CELLULAR TELEPHONE.
4. A REGIONAL TELEPHONE COMPANY IN THE MID-WESTERN U.S. WAS UNABLE TO PROVIDE A FEDERAL LAW ENFORCEMENT AGENCY WITH THE CONTENT AND DIALED NUMBER INFORMATION FROM A SUSPECTED DRUG TRAFFICKERS TELEPHONE AS A RESULT OF THE SUBJECTS USE OF CUSTOM CALLING FEATURES.
5. A CELLULAR SERVICE PROVIDER IN THE SOUTH WAS UNABLE TO COMPLY WITH A FEDERAL COURT-ORDER FOR DIALED NUMBER INFORMATION CONCERNING A FEDERAL PUBLIC CORRUPTION

INVESTIGATION DUE TO TECHNICAL LIMITATIONS.

IT IS IMPORTANT TO NOTE THAT THERE HAVE BEEN MANY INSTANCES WHERE COURT ORDERS HAVE NOT BEEN SOUGHT OR SERVED ON CARRIERS DUE TO LAW ENFORCEMENT'S AWARENESS OF THESE PRE-EXISTING IMPEDIMENTS, AND THEREFORE THEY WERE NOT TABULATED IN CONNECTION WITH THIS SURVEY. INCLUDED IN A RECENT LETTER FROM THE DIRECTOR OF A HIGH INTENSITY DRUG TRAFFICKING AREA (HIDTA) IT WAS NOTED THAT A FEDERAL LAW ENFORCEMENT AGENCY DID NOT PURSUE TWENTY-FIVE COURT ORDERS BECAUSE OF THE KNOWN INABILITIES OF THE CELLULAR SERVICE PROVIDER TO EFFECTUATE SUCH ORDERS.

HOWEVER, IT WOULD BE A MISTAKE TO ANALYZE AND RESPOND TO THIS PROBLEM SIMPLY BY ATTEMPTING TO COUNT THE SPECIFIC NUMBER OF COURT ORDERS FRUSTRATED OR DELAYED IN THE PAST. ALTHOUGH THEY CONVEY A SENSE OF THE PROBLEM, AND IDENTIFY SOME OF THE TECHNICAL PROBLEMS THAT ARE BEING ENCOUNTERED AS A RESULT OF RECENT TELECOMMUNICATIONS TECHNOLOGY ADVANCES, FOCUSING ON THESE NUMBERS AND TECHNOLOGIES ALONE IS TERRIBLY MISLEADING. FORTUNATELY, THE NUMBER OF COURT-ORDERED INTERCEPTIONS THAT HAVE BEEN IMPEDED BY TECHNOLOGY IS STILL SOMEWHAT LIMITED. HOWEVER, THE TELECOMMUNICATIONS TECHNOLOGIES THAT ARE EMERGING WILL LIKELY HAVE A MUCH GREATER AND MORE DEVASTATING IMPACT ON LAW ENFORCEMENT'S ABILITY TO CONDUCT COURT-ORDERED ELECTRONIC SURVEILLANCE IN THE FUTURE.

FBI/GOVERNMENT EFFORTS TO OBTAIN TELECOMMUNICATIONS INDUSTRY'S COOPERATION/SOLUTIONS

FOR ALMOST FOUR YEARS, THE GOVERNMENT HAS ATTEMPTED TO RESOLVE THE TECHNICAL ISSUES ASSOCIATED WITH COURT-ORDERED ELECTRONIC SURVEILLANCE BY MEETING WITH VARIOUS REPRESENTATIVES OF THE TELECOMMUNICATIONS INDUSTRY AT VIRTUALLY ALL CORPORATE LEVELS. HISTORICALLY, LAW ENFORCEMENT'S INTERFACE WITH THIS INDUSTRY HAS BEEN THROUGH THE SECURITY ORGANIZATION OF THE COMMON CARRIER. IT IS THIS INTERFACE THAT PREVIOUSLY HAS BEEN MOST KNOWLEDGEABLE OF LAW ENFORCEMENT'S ELECTRONIC SURVEILLANCE

REQUIREMENTS, AS THEY RECEIVE COURT ORDERS REQUIRING THEM TO ASSIST LAW ENFORCEMENT WITH THEIR ELECTRONIC SURVEILLANCE RESPONSIBILITIES. HOWEVER, IT WAS LEARNED IN 1990, DURING DISCUSSIONS WITH THE INDUSTRY, THAT THE SECURITY ENTITIES WITHIN THE COMMON CARRIER COMPANIES WERE NOT ROUTINELY INVOLVED IN THE INDUSTRY'S TECHNOLOGY PLANNING, DESIGN, AND DEVELOPMENT PROCESSES. AS A RESULT, LAW ENFORCEMENT'S NEEDS WERE NOT BEING INCORPORATED INTO THE CARRIERS' SYSTEM REQUIREMENTS.

IN AN ATTEMPT TO HAVE LAW ENFORCEMENT'S REQUIREMENTS CONSIDERED DURING THE INDUSTRY'S PLANNING PROCESSES, THE GOVERNMENT SYSTEMATICALLY MET WITH THE MOST SENIOR LEVELS OF THE TRADITIONAL COMMON CARRIERS AND BRIEFED THEM ABOUT THE DIFFICULTIES BEING ENCOUNTERED BY LAW ENFORCEMENT AND ABOUT OUR CONCERNS THAT FUTURE TECHNOLOGIES WOULD SEVERELY DIMINISH, IF NOT PRECLUDE, THIS CRITICAL INVESTIGATIVE TECHNIQUE. ALTHOUGH THESE EXECUTIVES APPEARED SUPPORTIVE OF LAW ENFORCEMENT'S GOALS, SEVERAL OF THEM INDICATED THAT WITHOUT SOME SORT OF MANDATE, SUCH AS LEGISLATION, THEIR COMPANIES COULD NOT UNILATERALLY INVEST TIME, MONEY, AND TECHNICAL RESOURCES IN DEVELOPING AND IMPLEMENTING SOLUTIONS, ESPECIALLY IF THERE WERE NO ASSURANCE THAT THEIR COMPETITORS WOULD DO SO.

ON JANUARY 15, 1992, THEN PRESIDENT BUSH AUTHORIZED THE JUSTICE DEPARTMENT TO PROCEED WITH A LEGISLATIVE INITIATIVE. ON MARCH 6, 1992, THE DIGITAL TELEPHONY LEGISLATION WAS ANNOUNCED, AND THE INDUSTRY RESPONSE WAS GENERALLY NEGATIVE, A POSITION THAT WAS AT VARIANCE WITH THAT EXPRESSED PREVIOUSLY BY A NUMBER OF THE REPRESENTATIVES OF THE TELECOMMUNICATIONS COMPANIES. ON MARCH 18, 1992, THEN ATTORNEY GENERAL WILLIAM BARR AND THEN FBI DIRECTOR WILLIAM S. SESSIONS SPONSORED AND CHAIRED A MEETING FOR ALL MAJOR INDUSTRY EXECUTIVES. IT WAS ATTENDED BY FOUR TELECOMMUNICATIONS EXECUTIVES, REPRESENTING THE INDUSTRY. DURING THIS MEETING, TELECOMMUNICATIONS EXECUTIVES ASSERTED THAT THE FBI HAD BEEN TALKING TO THE WRONG PEOPLE IN INDUSTRY (THE SECURITY OFFICERS, SENIOR EXECUTIVES, ETC.) AND THAT THE SOLUTION TO THESE PROBLEMS RESTED WITH THOSE UPPER/MID-LEVEL MANAGERS AND ENGINEERS

WHO OVERSAW DEVELOPMENT/IMPLEMENTATION OF THE TECHNOLOGIES IN QUESTION. THE ATTORNEY GENERAL AGREED TO AN INDUSTRY REQUEST THAT A TELECOMMUNICATIONS TECHNICAL COMMITTEE CONSISTING OF THE "RIGHT INDUSTRY PEOPLE" (PICKED BY THE CEOS) BE CREATED TO IDENTIFY TECHNICAL SOLUTIONS AND TO GET THE JOB DONE. IT WAS ALSO CLEARLY UNDERSTOOD THAT THE ADMINISTRATION AND LAW ENFORCEMENT WOULD CONTINUE TO PURSUE LEGISLATION.

AS A RESULT OF THE MARCH 18, 1992, MEETING, INDUSTRY REPRESENTATIVES MET WITH THE GOVERNMENT ON MARCH 26, 1992, TO BEGIN A PROCESS OF ESTABLISHING A TECHNICAL WORKING COMMITTEE TO ADDRESS TECHNICAL IMPEDIMENTS TO ELECTRONIC SURVEILLANCE. IN MAY OF 1992, AN AD HOC TECHNICAL WORKING GROUP BEGAN. THIS GROUP WAS LATER ORGANIZED AS THE ELECTRONIC COMMUNICATION SERVICE PROVIDERS COMMITTEE UNDER AN INDUSTRY ASSOCIATION NOW KNOWN AS THE ALLIANCE FOR TELECOMMUNICATIONS INDUSTRY SOLUTIONS (ATIS). THIS COMMITTEE CONSISTS OF REPRESENTATIVES OF ELECTRONIC COMMUNICATION SERVICE PROVIDERS (E.G. COMMON CARRIERS), TELECOMMUNICATIONS EQUIPMENT MANUFACTURERS, AND LAW ENFORCEMENT OFFICIALS, WHO ATTEND VOLUNTARILY AND WITH VARYING DEGREES OF REGULARITY AND INTEREST. AS A RESULT OF THIS PROCESS, OVER THE PAST TWO YEARS THERE HAS BEEN A BETTER UNDERSTANDING BY BOTH LAW ENFORCEMENT AND INDUSTRY REPRESENTATIVES OF THE ISSUES THAT EACH FACE WITH RESPECT TO ELECTRONIC SURVEILLANCE. HOWEVER, CONTRARY TO ASSERTIONS, NEW TELECOMMUNICATIONS TECHNOLOGIES WILL JEOPARDIZE LAW ENFORCEMENT'S SURVEILLANCE ABILITIES. THE ATIS CHAIRMAN HAS STATED IN A RECENT LETTER THAT THE ENTIRE COMMITTEE, NOT JUST ONE PARTICIPANT OR ONE GROUP OF PARTICIPANTS, NOW RECOGNIZES THE PROBLEMS AND IMPEDIMENTS THAT THESE TELECOMMUNICATIONS TECHNOLOGIES ARE CREATING FOR LAW ENFORCEMENT. A COPY OF OUR CORRESPONDENCE WITH THE ATIS CHAIRMAN IS ATTACHED AS AN EXHIBIT.

I SUPPORT CONTINUED DIALOGUE BETWEEN INDUSTRY AND LAW ENFORCEMENT. HOWEVER, IT MUST BE RECOGNIZED THAT THIS COMMITTEE PROCESS IS VOLUNTARY AND, AS SUCH, ONLY THOSE COMPANIES WHO ARE COMMITTED TO ASSISTING LAW ENFORCEMENT PARTICIPATE AND SUPPORT THIS EFFORT. SECOND, ONLY A HANDFUL OF THE OVER 2,000 COMPANIES

ATTEND. THIRD, NO IMPLEMENTABLE SOLUTIONS HAVE BEEN DEVELOPED SINCE DISCUSSIONS BEGAN ALMOST TWO YEARS AGO. FOURTH, COMMITTEE RESOLUTIONS ARE NON-BINDING AND IT IS NOT POSSIBLE TO SECURE A COMMITMENT FROM PARTICIPANTS TO IMPLEMENT ANY SOLUTIONS THAT MAY BE DEVELOPED IN THIS VOLUNTARY FORUM. FINALLY, AS IN ANY BUSINESS DECISION, IT IS RECOGNIZED THAT THERE WILL BE COSTS INCURRED BY INDUSTRY TO ACCOMMODATE LAW ENFORCEMENT'S REQUIREMENTS. THE ATIS CHAIRMAN HAS ALSO INDICATED THAT ANTITRUST AND OTHER LEGAL CONSIDERATIONS PRECLUDE DISCUSSIONS AND RESOLUTIONS TO THESE COST ISSUES. IN LIGHT OF THESE LIMITATIONS, THE ADMINISTRATION AND ALL OF LAW ENFORCEMENT HAVE CONCLUDED THAT THE COMMITTEE PROCESS IS NOT, AND CANNOT BE, A SUBSTITUTE FOR A LEGISLATIVE MANDATE TO ENSURE LAW ENFORCEMENT'S CONTINUED ABILITY TO CONDUCT COURT-AUTHORIZED ELECTRONIC SURVEILLANCE.

PRESIDENTIAL REVIEW DIRECTIVE (PRD)

IN APRIL 1993, PRESIDENT CLINTON DIRECTED THAT AN INTERAGENCY WORKING GROUP BE ESTABLISHED UNDER THE AUSPICES OF THE NATIONAL SECURITY COUNCIL (NSC) TO EXAMINE ADVANCED TELEPHONY AND TO CONSIDER ITS EFFECT AND IMPACT ON THE CONDUCT OF ELECTRONIC SURVEILLANCE BY OUR NATION'S LAW ENFORCEMENT AND INTELLIGENCE AGENCIES. AFTER AN IN-DEPTH EIGHT MONTH STUDY, THE NSC PROVIDED A NUMBER OF POLICY OPTIONS FOR THE VICE PRESIDENT AND APPROPRIATE CABINET OFFICIALS. AS A RESULT OF THEIR REVIEW OF THE OPTIONS, IT WAS UNANIMOUSLY DECIDED THAT COMPREHENSIVE LEGISLATION WAS THE ONLY EFFECTIVE WAY TO DEAL WITH THE "DIGITAL TELEPHONY" PROBLEM. FUNDAMENTAL TO THIS DECISION WAS THE BELIEF THAT IT WOULD BE UNACCEPTABLE FOR THE SAFETY OF THE AMERICAN PUBLIC TO BE IMPERILED, THE NATIONAL SECURITY ENDANGERED, AND EFFECTIVE LAW ENFORCEMENT ERODED THROUGH THE LOSS OR DIMINISHMENT OF THIS CRITICAL AND ESSENTIAL TOOL OF OUR NATION'S LAW ENFORCEMENT AND INTELLIGENCE AGENCIES.

PROPOSED LEGISLATION

THE PROPOSED LEGISLATION REPRESENTS, IN OUR ESTIMATION, THE ONLY RATIONAL AND VIABLE APPROACH TO SOLVING THE DIGITAL TELEPHONY PROBLEM IN A COMPREHENSIVE FASHION. ONLY THROUGH LEGISLATION CAN THE GOVERNMENT BE ASSURED THAT WITHIN A REASONABLE PERIOD OF TIME THE IMPEDIMENTS TO ELECTRONIC SURVEILLANCE WILL BE REMOVED AND OUR SOCIETY'S WINDOW OF VULNERABILITY CLOSED. WITHOUT ENACTMENT OF THE ADMINISTRATION'S PROPOSAL, ONE OF OUR MOST EFFECTIVE WEAPONS AGAINST NATIONAL AND INTERNATIONAL DRUG TRAFFICKING, TERRORISM, ESPIONAGE, ORGANIZED CRIME, AND SERIOUS VIOLENT CRIMES WILL BE SEVERELY AND ADVERSELY IMPACTED. WITHOUT ITS ENACTMENT, THE PUBLIC SAFETY, THE NATIONAL SECURITY, AND EFFECTIVE LAW ENFORCEMENT WILL BE IMPERILED.

THE PURPOSE OF THIS LEGISLATION IS TO MAINTAIN TECHNOLOGICAL CAPABILITIES COMMENSURATE WITH EXISTING STATUTORY AUTHORITY -- THAT IS, TO PREVENT ADVANCED TELECOMMUNICATIONS TECHNOLOGY FROM REPEALING DE FACTO THE STATUTORY AUTHORITY ALREADY CONFERRED BY THE CONGRESS. THE PROPOSED LEGISLATION EXPLICITLY STATES THAT THE LEGISLATION DOES NOT ENLARGE OR REDUCE THE GOVERNMENT'S AUTHORITY TO LAWFULLY INTERCEPT THE CONTENT OF COMMUNICATIONS OR INSTALL OR USE PEN REGISTER OR TRAP AND TRACE DEVICES PURSUANT TO COURT AUTHORIZATION. NEITHER DOES IT ALTER THE CURRENT DUTY OF THE SERVICE PROVIDER TO ASSIST LAW ENFORCEMENT AND RECEIVE PAYMENT FOR SUCH ASSISTANCE. NOR DOES IT ALTER EXISTING CAUSES OF ACTION, CIVIL LIABILITY, OR GOOD FAITH DEFENSES.

THE "PURPOSE" SECTION OF THE ACT INDICATES THAT THE ACT IS DESIGNED TO CLARIFY AND DEFINE THE RESPONSIBILITIES OF COMMON CARRIERS, PROVIDERS OF COMMON CARRIER SUPPORT SERVICES, AND TELECOMMUNICATIONS EQUIPMENT MANUFACTURERS. THEY WOULD BE REQUESTED TO PROVIDE THE ASSISTANCE REQUIRED TO ENSURE THAT GOVERNMENT AGENCIES CAN IMPLEMENT COURT ORDERS AND LAWFUL AUTHORIZATIONS TO INTERCEPT THE CONTENT OF WIRE AND ELECTRONIC COMMUNICATIONS AND ACQUIRE CALL SETUP INFORMATION (E.G., DIALED NUMBER INFORMATION), PURSUANT TO THE FEDERAL AND STATE ELECTRONIC

SURVEILLANCE AND PEN REGISTER AND TRAP AND TRACE STATUTES. THE "ASSISTANCE" REQUIREMENT THAT IS CLARIFIED AND MORE FULLY DEFINED IS NOT A NEW ONE, BUT RATHER A LONG-STANDING ONE, DATING BACK TO 1970. IN THE ORIGINAL ASSISTANCE PROVISION, CONGRESS EVIDENCED A CLEAR INTENT THAT LAWFUL COURT ORDERS SHOULD NOT BE FRUSTRATED DUE TO A SERVICE PROVIDER'S FAILURE TO PROVIDE NEEDED TECHNOLOGICAL ASSISTANCE AND FACILITIES. THE PROPOSED LEGISLATION CLARIFIES AND DEFINES THE NATURE AND EXTENT OF THE RESPONSIBILITY WHICH ARISES FROM THE UNEQUIVOCAL MANDATE OF THE 1970 LAW.

AN ADDITIONAL PURPOSE OF THE ACT IS TO IMPROVE COMMUNICATIONS PRIVACY PROTECTION FOR USERS OF CORDLESS TELEPHONES, CERTAIN RADIO-BASED DATA COMMUNICATIONS AND NETWORKS, COMMUNICATIONS TRANSMITTED USING CERTAIN PRIVACY-ENHANCING MODULATION TECHNIQUES, AND TO CLARIFY THE LAWFULNESS OF QUALITY CONTROL AND SERVICE PROVISION MONITORING OF ELECTRONIC COMMUNICATIONS ON A PAR WITH WIRE COMMUNICATIONS.

THE LEGISLATION SETS FORTH LAW ENFORCEMENT'S ELECTRONIC SURVEILLANCE REQUIREMENTS. THE REQUIREMENTS ARE, BY DESIGN, GENERIC IN NATURE AND ARE INTENDED TO PUT COMMON CARRIERS ON NOTICE AS TO NEEDS OF LAW ENFORCEMENT. THE GOVERNMENT PURPOSELY ESCHewed SETTING ANY TECHNICAL STANDARDS BECAUSE IT DOES NOT DESIRE TO "DICTATE" PARTICULAR TECHNOLOGICAL SOLUTIONS. IT IS THE GOVERNMENT'S POSITION THAT EACH COMMON CARRIER IS BEST POSITIONED AND QUALIFIED TO DETERMINE HOW IT WILL MEET THE REQUIREMENTS IN THE MOST COST-EFFECTIVE WAY.

THE ARTICULATION OF THESE REQUIREMENTS CONSTITUTES THE FIRST LEGISLATIVE LISTING OF LAW ENFORCEMENT'S ELECTRONIC SURVEILLANCE REQUIREMENTS. HOWEVER, MOST OF THESE REQUIREMENTS HAVE BEEN KNOWN TO THE MAJOR LOCAL EXCHANGE CARRIERS, INTEREXCHANGE CARRIERS, AND CELLULAR CARRIERS FOR QUITE SOME TIME.

IN BRIEF, THE REQUIREMENTS SPECIFY THAT COMMON CARRIERS MUST BE ABLE TO PROVIDE FORTHWITH, PURSUANT TO COURT ORDER OR LAWFUL AUTHORIZATION, THE CAPABILITY AND CAPACITY TO PERMIT THE

GOVERNMENT TO CONDUCT ELECTRONIC SURVEILLANCE, PEN REGISTER, AND TRAP AND TRACE INVESTIGATIONS EFFECTIVELY. COMMON CARRIERS ARE REQUIRED TO ENSURE THAT THERE IS AN ABILITY TO EXECUTE EXPEDITIOUSLY AND SIMULTANEOUSLY ALL COURT ORDERS AND LAWFUL AUTHORIZATIONS DIRECTED TO THEM. SECOND, THEY ARE REQUIRED TO ENSURE THAT THE CONTENT OF COMMUNICATIONS AND CALL SETUP INFORMATION (DIALING INFORMATION) CAN BE INTERCEPTED, ACQUIRED, AND PROVIDED TO THE LAW ENFORCEMENT AGENCY. IT MUST BE PROVIDED CONCURRENT WITH THE TRANSMISSION OF THE SUBJECT'S COMMUNICATION, TO THE EXCLUSION OF ANYONE ELSE'S COMMUNICATIONS OR DIALING INFORMATION, AND WITHOUT REGARD TO THE MOBILE NATURE OF THE FACILITY OR SERVICE THAT IS THE SUBJECT OF THE COURT ORDER OR LAWFUL AUTHORIZATION, REGARDLESS OF ANY FEATURES OFFERED BY THE COMMON CARRIER USED BY THE SUBSCRIBER WHO IS THE SUBJECT OF THE COURT ORDERED INTERCEPT. THIRD, THEY ARE REQUIRED TO ENSURE THAT COMMUNICATIONS CAN BE INTERCEPTED AND DIALING INFORMATION ACQUIRED UNOBTUSIVELY AND WITH A MINIMUM OF INTERFERENCE WITH ANY SUBSCRIBER'S TELECOMMUNICATIONS SERVICE. FINALLY, THEY ARE REQUIRED TO ENSURE THAT THE CONTENT OF COMMUNICATIONS AND THE DIALING INFORMATION CAN BE TRANSMITTED TO A LOCATION IDENTIFIED BY THE GOVERNMENT DISTANT FROM THE FACILITY THAT IS THE SUBJECT OF THE INTERCEPTION, FROM THE INTERCEPTION ACCESS POINT, AND FROM THE PREMISES OF THE COMMON CARRIER.

THE BASIS FOR THESE REQUIREMENTS IS EASY TO UNDERSTAND. INASMUCH AS COMMUNICATION INTERCEPTIONS AND DIALED NUMBER ACQUISITIONS INCREASINGLY WILL BE ACTIVATED FROM WITHIN COMMON CARRIER PREMISES, INCLUDING SWITCHING OFFICES, IT IS CRITICAL THAT THERE BE SUFFICIENT CAPACITY TO ACCOMMODATE COMPLETELY THE CONCOMITANT NEEDS OF ALL LAW ENFORCEMENT AND GOVERNMENT AGENCIES.

IT IS CRITICAL FOR LAW ENFORCEMENT AGENCIES TO BE ABLE TO INTERCEPT COMMUNICATIONS AND ACQUIRE DIALING INFORMATION CONCURRENTLY, SO THEY CAN RESPOND IMMEDIATELY TO LIFE-THREATENING CIRCUMSTANCES AND REACT PROMPTLY AND EFFECTIVELY TO CRIMINAL ACTIVITY IN TERMS OF MAKING NEEDED ARRESTS, SEIZING EVIDENCE, AND INTERDICTING CONTRABAND, SUCH AS DRUGS, ILLEGAL WEAPONS, AND

BOMBS. THIS REQUIREMENT ALSO IS IMPORTANT AND CRITICAL IN HELPING LAW ENFORCEMENT AGENCIES "MINIMIZE" THE MONITORING AND RECORDING OF NONCRIMINAL COMMUNICATIONS.

THE REQUIREMENT THAT COMMON CARRIERS HAVE THE ABILITY TO ISOLATE FOR LAW ENFORCEMENT THE COMMUNICATIONS AND DIALING INFORMATION OF THE SUBJECTS OF ELECTRONIC SURVEILLANCE TO THE EXCLUSION OF THE COMMUNICATIONS AND DIALING INFORMATION OF OTHER SUBSCRIBERS IS A BASIC AND A LONG-STANDING ONE. LAW ENFORCEMENT AGENCIES DO NOT WANT TO BE FACED WITH THE PROSPECT OF HAVING TO "SORT THROUGH" A TANGLE OF COMMUNICATIONS WHICH INCLUDE THE COMMUNICATIONS OF INNOCENT INDIVIDUALS WHO HAVE THE MISFORTUNE OF HAVING THEIR COMMUNICATIONS "BUNDLED" OR OTHERWISE COMMINGLED WITH THOSE CRIMINAL CONVERSATIONS OF THE SUBJECT OF COURT-ORDERED INTERCEPTION IN THE TELECOMMUNICATIONS TRANSMISSION PROCESS. (HOWEVER, IF THE "BUNDLING" OF COMMUNICATIONS IS BEING DONE BY THE SUBSCRIBER LAW ENFORCEMENT DOES NOT EXPECT THE COMMON CARRIER TO "UNBUNDLE" THESE COMMUNICATIONS. THIS ABILITY IS BEING CHALLENGED BY THE INCREASED USE OF DIGITAL TRANSPORT, MULTIPLEXING, AND FIBER OPTICS CLOSER TO THE PREMISES OF THE INTERCEPTION SUBJECT.

THE REQUIREMENT PERTAINING TO THE MOBILE NATURE OF SERVICES AND FEATURES DIRECTLY ADDRESSES THE SIGNIFICANT IMPEDIMENTS TO ELECTRONIC SURVEILLANCE BROUGHT ABOUT BY CELLULAR, PERSONAL COMMUNICATIONS SERVICES (PCS), AND OTHER EMERGING MOBILE SERVICES, AS WELL AS FEATURES AND SERVICES WHICH PERMIT SUBSCRIBERS TO PROGRAM OR OTHERWISE DIRECT COMMUNICATIONS TO ANY FACILITY THEY CHOOSE (E.G., "CALL FORWARDING" AND "FOLLOW ME SERVICE").

THE BASIS FOR THE REQUIREMENT THAT COMMUNICATIONS AND DIALING INFORMATION BE ACQUIRED UNOBTUSIVELY AND WITH A MINIMUM OF INTERFERENCE WITH ANY SUBSCRIBER'S SERVICE IS SELF EVIDENT. WITHOUT IT, ELECTRONIC SURVEILLANCE WOULD BE DETECTED BY THE SUBJECT OF THE INTERCEPT AND COMPROMISED.

THE REQUIREMENT THAT INTERCEPTED COMMUNICATIONS OR ACQUIRED DIALING INFORMATION BE RECEIVED AT A LOCATION IDENTIFIED

BY LAW ENFORCEMENT AGENCIES DISTANT FROM THE SUBJECT'S FACILITY, FROM THE INTERCEPTION POINT, AND FROM THE PREMISES OF THE COMMON CARRIER IS LIKEWISE NOT NEW AND MAINTAINS CURRENT OPERATING PROCEDURES. THIS REQUIREMENT IS FUNDAMENTALLY IMPORTANT, SINCE WITHOUT IT THE SAFETY OF LAW ENFORCEMENT OFFICERS AND GOVERNMENT EMPLOYEES WOULD BE PUT AT RISK, THE INTERCEPTION EASILY COULD BE COMPROMISED THROUGH DETECTION, AND THE EFFECTIVE EXECUTION OF THE SURVEILLANCE WOULD BE SIGNIFICANTLY DISRUPTED.

THE LEGISLATION CONTAINS A PROVISION ENTITLED "SYSTEMS SECURITY" WHICH IS INTENDED TO MAINTAIN THE HIGHEST LEVELS OF TELECOMMUNICATIONS PRIVACY AND SYSTEMS SECURITY. SINCE COMMUNICATION INTERCEPTIONS AND DIALING INFORMATION ACQUISITIONS INCREASINGLY WILL BE FACILITATED FROM WITHIN COMMON CARRIER PREMISES, INCLUDING SWITCHING FACILITIES AND NETWORK ELEMENTS, IT IS CRITICAL THAT THESE FACILITIES REMAIN HIGHLY SECURE. CONSEQUENTLY, LAW ENFORCEMENT WILL BE REQUIRED TO NOTIFY COMMON CARRIERS OF ANY INTERCEPTIONS THAT ARE TO BE EFFECTED WITHIN SUCH FACILITIES. FURTHER, COMMON CARRIERS WILL DESIGNATE INDIVIDUALS WHO EXCLUSIVELY WILL HAVE THE ABILITY TO ACTIVATE ALL SUCH INTERCEPTIONS FOR LAW ENFORCEMENT. LAW ENFORCEMENT AND OTHER GOVERNMENT AGENCIES ARE NOT SEEKING THE AUTHORITY OR ABILITY TO REMOTELY ACTIVATE INTERCEPTIONS WITHIN THE PREMISES OF A COMMON CARRIER IN A FASHION THAT BYPASSES PERSONNEL DESIGNATED BY COMMON CARRIER. ALL EXECUTIONS OF COURT ORDERS OR AUTHORIZATIONS WHICH REQUIRE ACCESS TO THE SWITCHING FACILITIES OR OTHER CARRIER PREMISES WILL BE MADE THROUGH THE INDIVIDUALS AUTHORIZED AND DESIGNATED BY THE COMMON CARRIER.

THE FOCUS OF COMPLIANCE IS UPON COMMON CARRIERS WITHIN WHOSE NETWORKS MOST OF THE ELECTRONIC SURVEILLANCE OCCURS AND WHERE MOST OF THE IMPEDIMENTS ARE ENCOUNTERED. COMPLIANCE IS SET FOR WITHIN THREE YEARS, A PERIOD OF TIME CONSIDERED TO BE REASONABLE FOR REMOVING THE IMPEDIMENTS. THE COVERAGE OF COMPLIANCE INCLUDES ONLY NEEDED MODIFICATIONS TO EXISTING SYSTEMS AND NETWORKS, AS WELL AS TO FUTURE SYSTEMS AND NETWORKS (THOSE FIELDIED AFTER THE THREE-YEAR COMPLIANCE PERIOD).

BECAUSE COMMON CARRIERS MUST RELY ON EQUIPMENT MANUFACTURERS AND SUPPORT SERVICE PROVIDERS, THE LEGISLATION PROVIDES THAT COMMON CARRIERS ARE TO CONSULT WITH THESE ENTITIES IN A TIMELY FASHION AND THAT THESE ENTITIES, IN TURN, SHALL MAKE AVAILABLE NEEDED EQUIPMENT AND SERVICES ON A TIMELY AND PRIORITY BASIS, AND AT A REASONABLE AND COST-EFFECTIVE CHARGE.

ENFORCEMENT OF THE LEGISLATION IS VESTED IN THE ATTORNEY GENERAL. THIS IS TO AVOID DISPARATE ENFORCEMENT ACTIONS THROUGHOUT THE COUNTRY IN WAYS THAT COULD BE BURDENSOME FOR COMMON CARRIERS. THE ATTORNEY GENERAL IS AUTHORIZED TO SEEK INJUNCTIVE RELIEF AGAINST COMMON CARRIERS, EQUIPMENT MANUFACTURERS, AND SUPPORT SERVICE PROVIDERS, AS WELL AS TO FILE CIVIL ACTIONS FOR FINES AGAINST COMMON CARRIERS. THE ATTORNEY GENERAL IS ALSO AUTHORIZED TO REQUEST ENFORCEMENT ASSISTANCE FROM THE FEDERAL COMMUNICATIONS COMMISSION. VIOLATORS ARE SUBJECT TO A CIVIL PENALTY OF \$10,000 PER DAY FOR EACH DAY IN VIOLATION. AS A PRACTICAL MATTER, IT IS NOT EXPECTED THAT THESE ENFORCEMENT REMEDIES AND ACTIONS WILL BE REQUIRED, PARTICULARLY WITH REGARD TO RESPONSIBLE COMMON CARRIERS. HOWEVER, WITH APPROXIMATELY 2,000 COMMON CARRIERS NOW IN THE TELECOMMUNICATIONS MARKETPLACE, THE PROSPECT THAT SOME WILL DISREGARD THESE REQUIREMENTS OR RESPOND TO THEM IN A DILATORY FASHION CANNOT BE DISREGARDED.

IN ORDER TO FACILITATE COMPLIANCE WITH THE PROVISIONS OF THIS LEGISLATION, THE ATTORNEY GENERAL IS ENCOURAGED TO CONSULT WITH THE FEDERAL COMMUNICATIONS COMMISSION AND COMMON CARRIER REPRESENTATIVES AND TO UTILIZE COMMON CARRIER STANDARDS BODIES, ASSOCIATIONS, OR OTHER SUCH ORGANIZATIONS TO DISCUSS DETAILS OF THE REQUIREMENTS AND COST-EFFECTIVE APPROACHES.

IN THE DEFINITION OF THE TERM "INTERCEPT," IT IS MADE CLEAR THAT THE LEGISLATION, AS A GENERAL RULE, DOES NOT MAKE COMMON CARRIERS RESPONSIBLE FOR DECIPHERING OR DECRYPTING ENCRYPTED COMMUNICATIONS. AS A GENERAL RULE, LAW ENFORCEMENT AGENCIES ASSUME THIS RESPONSIBILITY. COMMON CARRIERS ARE REQUIRED TO PROVIDE ONLY THE PLAINTEXT OF ENCRYPTED COMMUNICATIONS WHEN THE ENCRYPTION WAS PROVIDED BY THE COMMON

CARRIER AND THE COMMON CARRIER POSSESSES THE INFORMATION NECESSARY TO DECRYPT THE COMMUNICATION.

THE TERM "CALL SETUP INFORMATION" IS ESSENTIALLY THE DIALING INFORMATION ASSOCIATED WITH ANY COMMUNICATION WHICH IDENTIFIES THE ORIGIN AND DESTINATION OF A WIRE OR ELECTRONIC COMMUNICATION OBTAINED THROUGH THE USE OF A PEN REGISTER OR TRAP AND TRACE DEVICE PURSUANT TO COURT ORDER. IT DOES NOT INCLUDE ANY INFORMATION WHICH MIGHT DISCLOSE THE GENERAL LOCATION OF A MOBILE FACILITY OR SERVICE, BEYOND THAT ASSOCIATED WITH THE AREA CODE OR EXCHANGE OF THE FACILITY OR SERVICE. THERE IS NO INTENT WHATSOEVER, WITH REFERENCE TO THIS TERM, TO ACQUIRE ANYTHING THAT COULD PROPERLY BE CALLED "TRACKING" INFORMATION.

THE LEGISLATION INCLUDES SEVERAL PROVISIONS THAT ARE INTENDED TO IMPROVE COMMUNICATIONS PRIVACY. THESE INCLUDE THE CONFERRAL OF FULL PRIVACY PROTECTION FOR CORDLESS TELEPHONES, INCLUDING THOSE TRANSMISSIONS OCCURRING IN THE RADIO LINK BETWEEN THE TELEPHONE HANDSET AND BASE STATION. THIS PROVISION RECOGNIZES THAT NEWER GENERATIONS OF CORDLESS TELEPHONES TEND TO AFFORD GREATER PRIVACY PROTECTION TO USERS THAN THOSE PREVIOUSLY MARKETED, BECAUSE LAWFUL NETWORK MONITORING IS ALLOWED FOR ELECTRONIC AS WELL AS WIRE COMMUNICATIONS.

IT IS IMPORTANT TO UNDERSTAND THAT THIS LEGISLATION IS INTENDED TO STAND THE TEST OF TIME AND OVERCOME THE SHORTCOMINGS OF THE 1970 AMENDMENT. IT IS SPECIFICALLY DESIGNED TO DEAL INTELLIGENTLY AND COMPREHENSIVELY WITH CURRENT AND EMERGING FUTURE TELECOMMUNICATIONS TECHNOLOGIES AND TO PRECLUDE THE NEED FOR MUCH MORE RESTRICTIVE AND MORE COSTLY LEGISLATION IN FIVE OR TEN YEARS WHEN COURT-AUTHORIZED INTERCEPTIONS WOULD NO LONGER BE POSSIBLE DUE TO FURTHER TECHNOLOGY ADVANCES. ANY LEGISLATION THAT WOULD LIMIT ITS APPLICATION TO TECHNOLOGICAL IMPEDIMENTS ON A "PIECEMEAL" BASIS WOULD BE DISASTROUS. PIECEMEAL LEGISLATION WHICH DEALS ONLY WITH CURRENT PROBLEMS OR SOME OF THE PROBLEMS WOULD RESULT IN COMMON CARRIERS FULLY DEPLOYING NEW TECHNOLOGIES WHICH WOULD IMPEDE ELECTRONIC SURVEILLANCE AND WHICH WOULD CAUSE THE GOVERNMENT TO RETURN TO THE CONGRESS REPEATEDLY. IN THE

MEANTIME, THE PUBLIC SAFETY, THE NATIONAL SECURITY, AND EFFECTIVE LAW ENFORCEMENT WOULD BE HARMED AND THE COST OF REMOVING THOSE FUTURE IMPEDIMENTS WOULD BE PROHIBITIVE. INDEED, IN THIS REGARD, BAD LEGISLATION WOULD BE WORSE THAN NO LEGISLATION AT ALL.

WHAT THE LEGISLATION DOES NOT PROPOSE

MUCH OF THE CRITICISM DIRECTED TOWARD THE ADMINISTRATION'S PROPOSAL HAS BEEN MISLEADING OR INCORRECT. I WOULD LIKE TO CLARIFY FOR THE RECORD WHAT THE LEGISLATION DOES NOT PROPOSE.

NO CHANGE IN LEGAL AUTHORITY

FIRST, AS I PREVIOUSLY STATED, THE PROPOSED LEGISLATION DOES NOT SEEK TO EXPAND THE CURRENT LAWS AUTHORIZING THE INTERCEPTION OF WIRE OR ELECTRONIC COMMUNICATIONS. TO THE CONTRARY, THIS PROPOSAL SIMPLY SEEKS TO MAINTAIN LAW ENFORCEMENT'S ABILITY TO CONDUCT THE TYPES OF SURVEILLANCES CURRENTLY AUTHORIZED IN CHAPTERS 119 AND 206, TITLE 18, U.S.C.; THE FOREIGN INTELLIGENCE SURVEILLANCE ACT; AND THE LAWS IN 37 STATES, THE DISTRICT OF COLUMBIA, PUERTO RICO, AND THE U.S. VIRGIN ISLANDS. IN 1968, CONGRESS CAREFULLY CONSIDERED AND PASSED LEGISLATION SETTING FORTH THE EXACT PROCEDURE BY WHICH LAW ENFORCEMENT CAN OBTAIN COURT AUTHORIZATION TO CONDUCT ELECTRONIC SURVEILLANCE. THE STATUTE DEMANDS THAT LAW ENFORCEMENT USE ELECTRONIC SURVEILLANCE ONLY AS A TECHNIQUE OF LAST RESORT. REQUESTS FOR ELECTRONIC SURVEILLANCE RECEIVE RIGOROUS ADMINISTRATIVE AND JUDICIAL SCRUTINY AND ARE GRANTED ONLY AFTER A FEDERAL DISTRICT COURT JUDGE, OR HIS/HER STATE/LOCAL COUNTERPART, IS SATISFIED THAT ALL THE STATUTORY SAFEGUARDS HAVE BEEN MET AND ALL OTHER REASONABLE INVESTIGATIVE STEPS HAVE FAILED, OR ARE LIKELY TO FAIL. THE PROPOSED LEGISLATION WILL NOT CHANGE THIS.

FURTHERMORE, SERVICE PROVIDERS WILL NOT EXECUTE AN INTERCEPT WITHOUT THE REQUIRED COURT ORDER OR STATUTORY AUTHORIZATION. ANY ATTEMPT TO DO SO BY ANYONE, EITHER INSIDE THE GOVERNMENT OR THE PRIVATE SECTOR, WILL CONTINUE TO BE A VIOLATION

OF FEDERAL LAW AND THOSE INDIVIDUALS WILL BE PROSECUTED TO THE FULLEST EXTENT OF THE LAW.

IN ADDITION, THE PROPOSAL WILL NOT CHANGE WHO CONTROLS ACCESS TO THE COMMUNICATIONS TO BE INTERCEPTED. IN FACT, INTERCEPTION ACCESS POINTS INCREASINGLY ARE LIKELY TO BE ACTIVATED WITHIN THE COMMON CARRIER'S PREMISES, THEREBY SEVERELY LIMITING THE POTENTIAL FOR ILLEGAL WIRETAPPING. THE PROPOSAL WILL NOT OPEN THE DOOR TO EASY OR WHOLESAL WIRETAPPING, NOR DOES LAW ENFORCEMENT ENVISION A MARKED INCREASE IN THE NUMBER OF ELECTRONIC SURVEILLANCE COURT ORDERS THAT WILL BE SOUGHT OR AN INCREASE IN THE TYPES OF INVESTIGATIONS IN WHICH A COURT-AUTHORIZED INTERCEPTION CAN BE GRANTED. THE LEGISLATION DOES NOT, IN ANY WAY, RELAX THE ESTABLISHED STATUTORY AND COURT-IMPOSED REQUIREMENT FOR OBTAINING A COURT ORDER.

THIS PROPOSAL DOES NOT RESTRICT TECHNOLOGY. IT DEALS SOLELY WITH PRESERVING TECHNICAL CAPABILITIES. THE PROPOSED LEGISLATION SEEKS ONLY TO CLARIFY AND MORE CLEARLY DEFINE EXISTING LAW REGARDING THE "TECHNICAL ASSISTANCE" PROVISION BY MAKING IT APPLICABLE AND MEANINGFUL, REGARDLESS OF THE TECHNOLOGY EMPLOYED.

ENCRYPTION

THE PROPOSAL, IN ESSENCE, ONLY ADDRESSES THE TECHNOLOGICAL ISSUE CONCERNING ACCESS TO COMMUNICATIONS AND DOES NOT ALTER THE LEGAL REQUIREMENTS CURRENTLY ASSOCIATED WITH COURT-ORDERED INTERCEPTS. WITH MINOR EXCEPTION WHERE ENCRYPTION WAS PROVIDED BY THE COMMON CARRIER AND THE COMMON CARRIER POSSESS IN THE INFORMATION NECESSARY TO DECRYPT THE INFORMATION, THE LEGISLATION DOES NOT ADDRESS THE ISSUE OF ENCRYPTION. WHILE ENCRYPTION CERTAINLY POSES A PROBLEM FOR LAW ENFORCEMENT, THIS LEGISLATIVE PROPOSAL FOCUSES ONLY ON THE ISSUE OF INTERCEPTION ACCESS WITHIN ADVANCED COMMUNICATIONS NETWORKS. THE TOPIC OF ACCESS WITHIN ADVANCED TELECOMMUNICATIONS NETWORKS IS DISTINCT FROM ENCRYPTION AND POSES AN IMMEDIATE AND CRITICAL PROBLEM FOR LAW ENFORCEMENT FOR WHICH WE ARE NOW SEEKING A LEGISLATIVE SOLUTION.

NETWORK SECURITY AND RELIABILITY

SOME HAVE RAISED CONCERNS REGARDING THE IMPACT THIS LEGISLATION MIGHT HAVE ON NETWORK SECURITY AND RELIABILITY. CERTAIN SPECIAL INTEREST SPOKESPERSONS HAVE ASSERTED THAT THE LEGISLATION WILL MAKE IT EASIER FOR ANYONE, FROM COMPUTER HACKERS TO FOREIGN SPIES, TO ACCESS AN INDIVIDUAL'S COMMUNICATIONS. THESE FEARS ARE UNFOUNDED AND MISPLACED. FIRST OF ALL, JUST AS NETWORK MAINTENANCE AND AUDIT ACCESS CAN BE ACCOMPLISHED WITH FULL REGARD FOR NETWORK AND SYSTEM SECURITY, SO ALSO CAN LAW ENFORCEMENT'S ELECTRONIC SURVEILLANCE ACCESS BE ACCOMPLISHED WITH THE SAME HIGH REGARD FOR SECURITY AND PRIVACY. SECOND, THE PROPOSED LEGISLATION INCLUDES A "SYSTEMS SECURITY" PROVISION WHICH MEANS THAT ONLY DESIGNATED TELEPHONE COMPANY EMPLOYEES WILL ACTIVATE INTERCEPTIONS WHICH ORIGINATE WITHIN TELEPHONE COMPANY PREMISES. THIRD, UNAUTHORIZED ACCESS TO COMMUNICATIONS REMAINS A SERIOUS CRIME WHICH IS ADDRESSED IN THE CURRENT ELECTRONIC SURVEILLANCE STATUTES. ANY UNAUTHORIZED INDIVIDUAL OR GROUP BREACHING COMMUNICATIONS SECURITY AND PRIVACY IS SUBJECT TO PROSECUTION TO THE FULLEST EXTENT OF THE LAW. FOURTH, THIS PROPOSAL WILL NOT INTRODUCE ANY VULNERABILITIES INTO SYSTEMS THAT ARE NOT ALREADY PRESENT. AS TECHNOLOGY EVOLVES AND AS ANY NEW FEATURES AND SERVICES ARE INTRODUCED, INDUSTRY WILL NECESSARILY PLAN NETWORK SECURITY MEASURES AND COUNTERMEASURES EARLY IN THE DESIGN PHASE AND ADDRESS INTENSIVELY THE ARCHITECTURAL DESIGN FOR NETWORK SECURITY.

THE PROPOSED LEGISLATION FITS WELL WITHIN THE CONTEXT OF THESE ACTIVITIES. BY REQUIRING COMMON CARRIERS TO DEVELOP LAW ENFORCEMENT ACCESS SOLUTIONS WITHIN THEIR OWN NETWORKS, WE ARE BEST ASSURING APPROPRIATE SECURITY. THEREFORE, CONTRARY TO MANY PUBLIC STATEMENTS MADE ON THE SUBJECT, LAW ENFORCEMENT IS NOT SEEKING TO BUILD "BACK DOORS" TO SNEAK INTO COMMON CARRIERS' SYSTEMS. THE PROPOSED LEGISLATION IS NOT SOME DREADED ORWELLIAN PROPHECY COME TRUE. RATHER, THIS LEGISLATIVE PROPOSAL REPRESENTS A RECOGNITION OF LEGITIMATE LAW ENFORCEMENT NEEDS AND A DESIRE TO PROTECT THE AMERICAN PEOPLE.

TO SUPPORT NORMAL OPERATIONS, SERVICE PROVIDERS MUST MANAGE AND MAINTAIN THEIR NETWORKS. THIS IS TERRIBLY IMPORTANT TO THE FBI JUST AS IT IS FOR EVERYONE. LAW ENFORCEMENT ELECTRONIC SURVEILLANCE INTERCEPTION ACCESS TO COMMUNICATIONS WILL BE A STRINGENTLY CONTROLLED EXTENSION OF THE SYSTEM'S FEATURES. WITH ADEQUATE PLANNING, THE INTEGRATION OF LAW ENFORCEMENT'S NEEDS SHOULD BE EASILY ACCOMMODATED WITHIN THE REQUIREMENTS FOR NETWORK SECURITY. TO FURTHER ENHANCE THE PUBLIC'S CONFIDENCE IN THE SECURITY OF OUR COMMUNICATIONS NETWORKS, SUBCOMMITTEE STAFF HAVE RAISED WITH US THE ISSUE OF IMPOSING REPORTING AND AUDITING REQUIREMENTS ON COMMON CARRIES CONCERNING THEIR IMPLEMENTATION OF AUTHORIZED INTERCEPTS. WE ARE SUPPORTIVE OF SUCH REQUIREMENTS.

EFFECTS ON NETWORK DESIGN AND TECHNOLOGY

ANOTHER CONCERN THAT HAS BEEN RAISED IS THE POSSIBLE NEGATIVE IMPACT THIS LEGISLATION MIGHT HAVE ON NETWORK DESIGN AND TECHNOLOGY, REQUIRING A BROAD RE-ENGINEERING OF THE NETWORK COMPONENTS. THE PROPOSED LEGISLATION DOES NOT REQUIRE COMMON CARRIERS TO DESIGN THEIR SYSTEMS IN ANY ONE, PARTICULAR WAY. THE PROPOSAL SIMPLY REQUIRES THAT COMMON CARRIERS RESPOND TO THE GENERIC REQUIREMENTS OF LAW ENFORCEMENT AND PROVIDE LAW ENFORCEMENT WITH INTERCEPTION ACCESS AND THE CAPABILITY AND CAPACITY TO INTERCEPT WIRE AND ELECTRONIC COMMUNICATIONS, IN REAL TIME, WHEN AUTHORIZED BY LAW.

THIS LEGISLATION ALSO DOES NOT PROPOSE THAT INDUSTRY DESIGN SYSTEMS WITH THE ABILITY TO WIRETAP AS THE "DESIGN GOAL." LAW ENFORCEMENT IS SIMPLY REQUIRING COMMON CARRIERS TO CRAFT APPROPRIATE SOLUTIONS THAT INTERFACE WITH THEIR NETWORKS' DESIGNS. INDUSTRY IS IN THE BEST POSITION TO DEVELOP REASONABLE AND COST-EFFECTIVE SOLUTIONS AND, AT THE SAME TIME, MAINTAIN THE SECURITY AND RELIABILITY OF THE NETWORKS.

FURTHERMORE, WE ARE UNAWARE OF ANY AUTHORITATIVE

INDUSTRY STATEMENT THAT THESE REQUIREMENTS WOULD SIGNIFICANTLY DELAY DEVELOPMENT OF NEW TECHNOLOGIES.

ADDITIONALLY, THIS LEGISLATION DOES NOT PROHIBIT OR IMPEDE THE DEPLOYMENT OF NEW TELECOMMUNICATIONS TECHNOLOGIES. ADVANCED TECHNOLOGIES SUPPORT A NUMBER OF FEATURES THAT MAKE SYSTEMS MORE INTELLIGENT. THE BASIC TECHNOLOGY UNDERPINNING THE INTRODUCTION OF ADVANCED FEATURES AND SERVICES, WHICH OFTEN IMPEDE ELECTRONIC SURVEILLANCE, LIKELY WILL OFFER SOLUTIONS TO THESE VERY PROBLEMS.

LAW ENFORCEMENT'S REQUIREMENTS WILL NOT DICTATE THE COURSE OR PACE OF TECHNOLOGY. HOWEVER, WITH THIS LEGISLATION, OUR REQUIREMENTS INTENTIONALLY WILL BE INCLUDED, RATHER THAN EXCLUDED, IN THE DEVELOPMENT OF NEW TECHNOLOGY IN MUCH THE SAME FASHION THAT OTHER LEGISLATION REQUIRES NEW TECHNOLOGIES AND PRODUCTS TO TAKE PUBLIC SAFETY INTO ACCOUNT.

COMPETITIVENESS

ANOTHER ISSUE RAISED PERTAINS TO THE EFFECT OF THE LEGISLATION ON AMERICAN COMPETITIVENESS. THE PROPOSED LEGISLATION WILL NOT IN ANY FASHION ADVERSELY AFFECT COMPETITIVENESS. DOMESTICALLY, THE PROPOSED LEGISLATION WOULD MEAN THAT ALL 2,000 COMMON CARRIERS WOULD COMPETE ON A "LEVEL PLAYING FIELD" BECAUSE ALL PROVIDERS WOULD BE REQUIRED TO MEET THE SAME ELECTRONIC SURVEILLANCE SPECIFICATIONS. THE PROPOSED LEGISLATION DOES NOT PROHIBIT U.S. MANUFACTURERS OR INTERNATIONAL SERVICE PROVIDERS FROM DEVELOPING OR DEPLOYING EQUIPMENT OR SERVICE FEATURES FOR SALE OUTSIDE THE UNITED STATES THAT ARE DIFFERENT FROM THAT REQUIRED PURSUANT TO THE PROPOSED LEGISLATION. THIS PROPOSAL ONLY APPLIES TO COMMON CARRIER COMMUNICATIONS SERVICES DEPLOYED WITHIN THE UNITED STATES. IF ANYTHING, THIS LEGISLATION COULD PROVIDE U.S. INDUSTRY WITH A COMPETITIVE EDGE. OTHER DEMOCRATIC NATIONS WILL VERY LIKELY WANT TELECOMMUNICATIONS SYSTEMS AND EQUIPMENT THAT PRECLUDE SERVICE PROVIDERS FROM DEVELOPING OR DEPLOYING EQUIPMENT OR SERVICE FEATURES NOT CAPABLE OF INTERCEPT.

PRIVACY-BASED OBJECTIONS

A SPOKESPERSON FOR THE AMERICAN CIVIL LIBERTIES UNION (ACLU) HAS STATED ON NUMEROUS OCCASIONS THAT THE ACLU OPPOSES THE PROPOSED LEGISLATION BECAUSE IT WOULD ALLOW LAW ENFORCEMENT TO MAINTAIN TECHNICAL CAPABILITIES COMMENSURATE WITH EXISTING FEDERAL AND STATE LEGAL AUTHORITIES. THIS IS BECAUSE THE ACLU OPPOSES THE EXISTING LEGAL AUTHORITIES -- THOSE FOUND IN THE TITLE III AND FISA STATUTES, AS IT PERSISTS IN THE ERRONEOUS POSITION THAT WIRETAPPING IS UNCONSTITUTIONAL PER SE. THIS RADICAL POSITION IS IN FLAT OPPOSITION TO THE POLICY POSITIONS AND THE CONSTITUTIONAL ANALYSES OF THE EXECUTIVE, LEGISLATIVE, AND JUDICIAL BRANCHES OF BOTH THE FEDERAL AND STATE GOVERNMENTS. THE UNITED STATES SUPREME COURT HELD LONG AGO THAT THE TITLE III WIRETAP STATUTE IS CONSTITUTIONAL. SEE UNITED STATES V. DONOVAN, 429 U.S. 413 (1977).

PRIVACY IS PROTECTED IN THE FEDERAL AND STATE ELECTRONIC SURVEILLANCE STATUTES BY REQUIRING LAW ENFORCEMENT AGENCIES' ADHERENCE TO A NUMBER OF LEGISLATIVELY-CREATED PROTECTIONS THAT FAR EXCEED THE FOURTH AMENDMENT REQUIREMENTS RELATING TO COURT ORDERS BASED UPON PROBABLE CAUSE.

IN FACT, THE PROPOSED LEGISLATION CONTAINS A NUMBER OF PRIVACY-ENHANCING PROVISIONS, SUCH AS EXTENDING FULL PRIVACY PROTECTION TO CORDLESS TELEPHONES, RADIO-BASED ELECTRONIC COMMUNICATIONS, AND COMMUNICATIONS TRANSMITTED USING PRIVACY-ENHANCING MODULATION TECHNIQUES.

THE FALSE "TRANSACTIONAL DATA SCARE"

THE DIGITAL PRIVACY AND SECURITY WORKING GROUP (DPSWG) HAS ATTEMPTED TO INTERJECT A FALSE "TRANSACTIONAL DATA SCARE" INTO THE CURRENT DISCUSSION OF THE NEED FOR LEGISLATION THAT WILL ALLOW LAW ENFORCEMENT TO MAINTAIN ITS ELECTRONIC SURVEILLANCE AND PEN REGISTER/TRAP AND TRACE TECHNICAL CAPABILITIES COMMENSURATE WITH EXISTING LAW.

IN A LETTER TO ME, DATED MARCH 11, 1994, A COPY OF

WHICH WAS SENT DIRECTLY TO THE CHAIRMEN, THE DPSWG FALSELY ALLEGES THAT WE ARE SEEKING TO "DICTATE TO INDUSTRY" A NEW CAPABILITY TO ACQUIRE "MINUTE-BY-MINUTE SURVEILLANCE OF INDIVIDUALS" THROUGH TRANSACTIONAL DATA. THIS IS A FALSE ISSUE FOR A NUMBER OF REASONS.

FIRST, AS IS CLEARLY SET FORTH IN THE "PURPOSE" SECTION OF THE PROPOSED LEGISLATION, THE INTENT OF THE LEGISLATION IS TO MAINTAIN EXISTING TECHNICAL CAPABILITIES AND TO "CLARIFY AND DEFINE THE RESPONSIBILITIES OF COMMON CARRIERS ... TO PROVIDE THE ASSISTANCE REQUIRED TO ENSURE THAT GOVERNMENT AGENCIES CAN IMPLEMENT COURT ORDERS AND LAWFUL AUTHORIZATIONS TO INTERCEPT THE CONTENT OF WIRE AND ELECTRONIC COMMUNICATIONS AND ACQUIRE CALL SETUP INFORMATION UNDER CHAPTERS 119 AND 206 OF TITLE 18 AND CHAPTER 36 OF TITLE 50." (EMPHASIS ADDED.) THESE CHAPTERS HAVE NOTHING TO DO WITH "TRANSACTIONAL INFORMATION" UNDER OUR FEDERAL ELECTRONIC SURVEILLANCE AND PRIVACY LAWS. ALL TELECOMMUNICATIONS "TRANSACTIONAL" INFORMATION IS ALREADY PROTECTED BY FEDERAL LAW AND IS EXCLUSIVELY DEALT WITH IN CHAPTER 121 OF TITLE 18 OF THE UNITED STATES CODE ("STORED WIRE AND ELECTRONIC COMMUNICATIONS AND TRANSACTIONAL RECORDS ACCESS"). THE PROPOSED LEGISLATION DOES NOT RELATE TO CHAPTER 121 OF TITLE 18.

SECOND, UNDER FEDERAL LAW, CONGRESS TREATS LAW ENFORCEMENT'S USE OF PEN REGISTERS AND DIALING INFORMATION DIFFERENTLY THAN "TRANSACTIONAL INFORMATION" -- SUCH AS DETAILED TELEPHONE BILLING INFORMATION. THE DIALING INFORMATION DERIVED FROM A PEN REGISTER IS OBTAINED BY LAW ENFORCEMENT AND IS LIMITED TO A SPECIFIC TELEPHONE LINE AND NUMBER. ON THE OTHER HAND, TRANSACTIONAL BILLING INFORMATION IS COMPILED BY TELEPHONE COMPANIES AND CAPTURES BILLING INFORMATION FROM EVERY TELEPHONE A SUBSCRIBER MAY USE DURING THE BILLING PERIOD, SUCH AS CREDIT CARD CALLS, COLLECT CALLS, OPERATOR ASSISTED CALLS, AND THIRD NUMBER BILLING INFORMATION WHICH ARE ASSOCIATED WITH ALL THE DIFFERENT TELEPHONES A SUBSCRIBER MAY USE.

THIRD, CONGRESS HAS ENACTED LEGISLATION THAT REQUIRES LAW ENFORCEMENT TO OBTAIN A COURT ORDER IN ORDER TO OBTAIN "CALL

SETUP INFORMATION" THROUGH THE USE OF A PEN REGISTER OR TRAP AND TRACE DEVICE, BASED UPON A CERTIFICATION OF AN ATTORNEY FOR THE GOVERNMENT THAT THE INFORMATION LIKELY TO BE OBTAINED IS RELEVANT TO AN ONGOING CRIMINAL INVESTIGATION. SUCH COURT ORDERS LAST FOR UP TO SIXTY DAYS. ANY RENEWAL REQUIRES THE APPROVAL OF AN APPROPRIATE JUDGE. ON THE OTHER HAND, CONGRESS HAS LEGISLATED THAT "TRANSACTIONAL INFORMATION" CAN BE OBTAINED THROUGH A NUMBER OF LEGAL PROCESSES, INCLUDING SUBPOENAS, WITHOUT RESORT TO COURT ORDERS. SUBPOENAS FOR TRANSACTIONAL INFORMATION TYPICALLY COVER PERIODS OF SIX MONTHS OR LONGER. IN ANY EVENT, LAW ENFORCEMENT IS NOT AUTHORIZED TO OBTAIN NONCRIMINAL, IRRELEVANT INFORMATION ABOUT ANY INDIVIDUAL, AND ANY ACQUISITION OF TRANSACTIONAL INFORMATION OR DIALING-TYPE INFORMATION MUST BE GROUNDED IN RELEVANCY TO A CRIMINAL INVESTIGATION OR INQUIRY.

FOURTH, THE LETTER INDICATES THAT ENACTMENT OF THIS LEGISLATION, WITH REGARD TO MAINTAINING OUR ABILITY TO LAWFULLY ACQUIRE CALL SETUP (DIALING) INFORMATION PURSUANT TO COURT ORDER, WILL SOMEHOW PERMIT LAW ENFORCEMENT TO ACQUIRE SOME NEW INFORMATION THAT IS NOT NOW AVAILABLE. THAT IS SIMPLY UNTRUE. THIS LEGISLATION ENSURES A MAINTENANCE OF THE STATUS QUO AS IT RELATES TO LEGAL AUTHORITIES UNDER CHAPTERS 119 AND 206 OF TITLE 18 AND CHAPTER 36 OF TITLE 50, AND AS IT RELATES TO THE TYPES OF INFORMATION OBTAINABLE THROUGH PEN REGISTER AND TRAP AND TRACE DEVICES USED PURSUANT TO THE COURT ORDER.

FIFTH, UNLIKE THE GOVERNMENT'S PROPOSED LEGISLATION, WHICH SPECIFICALLY ASSERTS NO INTENTION TO ALTER THE EXISTING LAWS REGARDING THE CONDUCT OF ELECTRONIC SURVEILLANCE AND THE INSTALLATION AND USE OF PEN REGISTER AND TRAP AND TRACE DEVICES, THE DPSWG, BY INTERJECTING A FALSE TRANSACTIONAL DATA SCARE, IS APPARENTLY SEEKING TO REPEAL CHAPTER 206 OF TITLE 18 AND THE PEN REGISTER AND TRAP AND TRACE AUTHORIZATIONS FOUND IN CHAPTER 36 OF TITLE 50. AS EXPLAINED ABOVE, CALL SETUP INFORMATION (THAT IS DIALING INFORMATION) IS OBTAINED THROUGH THE USE OF PEN REGISTER AND TRAP AND TRACE DEVICES. IN THE DPSWG LETTER REFERRED TO

ABOVE, IT STATES: "LEGISLATION SHOULD APPLY TO "CALL SETUP INFORMATION" ONLY WHEN THAT INFORMATION IS INCIDENT TO A WARRANT ISSUED FOR WIRE, ORAL, OR ELECTRONIC COMMUNICATIONS AS SET FORTH IN 18 U.S.C. 2518 [TITLE III]." TO ACCEPT THIS RADICAL POSITION ON PRIVACY WOULD MEAN, FOR EXAMPLE, THAT ANYTIME AN FBI AGENT SIMPLY SOUGHT TO ACQUIRE A TELEPHONE NUMBER DIALED BY A CRIMINAL SUBJECT THROUGH THE USE OF A PEN REGISTER, HE/SHE SHOULD BE REQUIRED BY LAW TO DRAFT A 30-40 PAGE TITLE III AFFIDAVIT, AND SEND IT TO WASHINGTON, D.C., FOR THE DEPUTY ASSISTANT ATTORNEY GENERAL OF THE CRIMINAL DIVISION TO REVIEW AND AUTHORIZE, BEFORE TAKING IT TO A FEDERAL DISTRICT COURT JUDGE FOR REVIEW AND APPROVAL. FRANKLY, SUCH A NOTION IS ABSURD AND IS WILDLY INCONSISTENT WITH CURRENT LAW.

ALLEGATIONS OF "TRACKING" PERSONS

LAW ENFORCEMENT'S REQUIREMENTS SET FORTH IN THE PROPOSED LEGISLATION INCLUDE AN ABILITY TO ACQUIRE "CALL SETUP INFORMATION." THIS INFORMATION RELATES TO DIALING TYPE INFORMATION -- INFORMATION GENERATED BY A CALLER WHICH IDENTIFIES THE ORIGIN, DURATION, AND DESTINATION OF A WIRE OR ELECTRONIC COMMUNICATION, THE TELEPHONE NUMBER OR SIMILAR COMMUNICATION ADDRESS. SUCH INFORMATION IS CRITICAL TO LAW ENFORCEMENT AND, HISTORICALLY, HAS BEEN ACQUIRED THROUGH USE OF PEN REGISTER OR TRAP AND TRACE DEVICES PURSUANT TO COURT ORDER.

SEVERAL PRIVACY-BASED SPOKESPERSONS HAVE CRITICIZED THE WORDING OF THE DEFINITION REGARDING THIS LONG-STANDING REQUIREMENT, ALLEGING THAT THE GOVERNMENT IS SEEKING A NEW, PERVASIVE, AUTOMATED "TRACKING" CAPABILITY. SUCH ALLEGATIONS ARE COMPLETELY WRONG.

SOME CELLULAR CARRIERS DO ACQUIRE INFORMATION RELATING TO THE GENERAL LOCATION OF A CELLULAR TELEPHONE FOR CALL DISTRIBUTION ANALYSIS PURPOSES. HOWEVER, THIS INFORMATION IS NOT THE SPECIFIC TYPE OF INFORMATION OBTAINED FROM "TRUE" TRACKING DEVICES, WHICH CAN REQUIRE A WARRANT OR COURT ORDER WHEN USED TO TRACK WITHIN A PRIVATE LOCATION NOT OPEN TO PUBLIC VIEW. SEE

UNITED STATES V. KARO, 468 U.S. 705, 714 (1984). EVEN WHEN SUCH GENERALIZED LOCATION INFORMATION, OR ANY OTHER TYPE OF "TRANSACTIONAL" INFORMATION, IS OBTAINED FROM COMMUNICATIONS SERVICE PROVIDERS, COURT ORDERS OR SUBPOENAS ARE REQUIRED AND ARE OBTAINED.

IN ORDER TO MAKE CLEAR THAT THE ACQUISITION OF SUCH INFORMATION IS NOT BEING SOUGHT THROUGH THE USE OF A PEN REGISTER OR TRAP AND TRACE DEVICE, AND IS NOT INCLUDED WITHIN THE TERM "CALL SETUP INFORMATION," WE ARE PREPARED TO ADD A CONCLUDING PHRASE TO THIS DEFINITION TO EXPLICITLY CLARIFY THE POINT: "..., EXCEPT THAT SUCH INFORMATION [CALL SETUP INFORMATION] SHALL NOT INCLUDE ANY INFORMATION THAT MAY DISCLOSE THE PHYSICAL LOCATION OF A MOBILE FACILITY OR SERVICE BEYOND THAT ASSOCIATED WITH THE NUMBER'S AREA CODE OR EXCHANGE."

SUMMARY

IN SUMMARY, IT IS MY VIEW THAT THE DIGITAL TELEPHONY ISSUE IS THE NUMBER ONE LAW ENFORCEMENT, PUBLIC SAFETY, AND NATIONAL SECURITY ISSUE FACING US TODAY. THE MAINTENANCE OF AN EFFECTIVE ELECTRONIC SURVEILLANCE CAPABILITY IS ESSENTIAL TO OUR NATION'S LAW ENFORCEMENT AND INTELLIGENCE AGENCIES. THIS INVESTIGATIVE TECHNIQUE IS A UNIQUE AND INDISPENSABLE WEAPON AGAINST NATIONAL AND INTERNATIONAL DRUG-TRAFFICKING ORGANIZATIONS, ORGANIZED CRIME SYNDICATES, TERRORIST GROUPS, AND VIOLENT CRIMINAL CONSPIRACIES. WITHOUT AN EFFECTIVE ELECTRONIC SURVEILLANCE CAPABILITY, OUR LAW ENFORCEMENT AND INTELLIGENCE AGENCIES WILL NOT BE ABLE TO PROTECT THE PUBLIC ADEQUATELY OR ACQUIRE THE EVIDENCE NEEDED TO PUT SOME OF SOCIETY'S MOST DANGEROUS FELONS IN JAIL. RECENT EFFORTS TO ENSURE SUBSTANTIAL JAIL TIME FOR VIOLENT, HARDENED CRIMINALS WILL BE UNDERCUT, IF WE IN LAW ENFORCEMENT FIRST CANNOT IDENTIFY THEM, ARREST THEM, AND OBTAIN THE COMPELLING EVIDENCE REQUIRED TO SECURE THEIR CONVICTIONS.

AS YOU ARE AWARE, AFTER AN EXTENSIVE REVIEW OF THIS

SERIOUS PROBLEM THE ADMINISTRATION HAS CONCLUDED THAT FEDERAL LEGISLATION IS THE ONLY VIABLE MEANS OF SOLVING THE SO-CALLED "DIGITAL TELEPHONY" PROBLEM. THE TECHNOLOGICAL IMPEDIMENTS TO COURT-ORDERED ELECTRONIC SURVEILLANCE, WHICH ARE THE UNINTENDED BY-PRODUCTS OF ADVANCED DIGITAL TELEPHONY, CONSTITUTE A MAJOR NATIONWIDE OBSTACLE TO EFFECTIVE LAW ENFORCEMENT. TO DATE, NUMEROUS COURT ORDERS HAVE BEEN FRUSTRATED, IN WHOLE OR IN PART, BY THESE IMPEDIMENTS. LEFT UNADDRESSED, THIS PROBLEM WILL SOON GROW TO DANGEROUS PROPORTIONS. THE FEDERAL BUREAU OF INVESTIGATION AND THE ENTIRE FEDERAL, STATE, AND LOCAL LAW ENFORCEMENT COMMUNITY ARE COMPLETELY UNIFIED IN OUR ASSESSMENT THAT IMPEDIMENTS WHICH HINDER OR PRECLUDE COURT-ORDERED ELECTRONIC SURVEILLANCE MUST NOT BE ALLOWED TO STAND.

THE DECISION TO PRESS FOR LEGISLATION WAS NOT REACHED LIGHTLY. OVER THE LAST FOUR YEARS, WE HAVE MADE SUBSTANTIAL EFFORTS TO RESOLVE THIS MATTER THROUGH NUMEROUS MEETINGS WITH LEADERS IN THE TELECOMMUNICATIONS INDUSTRY. INCLUDED IN THESE EFFORTS HAS BEEN A LAW ENFORCEMENT/INDUSTRY TECHNICAL WORKING GROUP WHICH WAS SPECIFICALLY INSTITUTED BY INDUSTRY TO "SOLVE THE PROBLEM." EVEN THOUGH WE HAVE MET FOR NEARLY TWO YEARS (AND HAVE MUTUALLY BENEFITTED FROM THE DISCUSSIONS), THERE IS NO MECHANISM FOR ASSURING THE TIMELY, COMPREHENSIVE DEVELOPMENT AND IMPLEMENTATION OF THE REQUIRED TECHNOLOGICAL SOLUTIONS. IN FACT, THE CHAIRMAN OF THE INDUSTRY TECHNICAL WORKING GROUP ACKNOWLEDGES THIS FUNDAMENTAL SHORTCOMING AND PROBLEM. OBTAINING THESE SOLUTIONS CAN NO LONGER BE LEFT TO CHANCE. FEDERAL LEGISLATION REPRESENTS THE ONLY REALISTIC PROSPECT FOR OBTAINING, WITH CERTAINTY, THE TIMELY AND COMPREHENSIVE DEVELOPMENT AND IMPLEMENTATION OF THE REQUIRED TECHNOLOGICAL SOLUTIONS BY THE TELECOMMUNICATIONS INDUSTRY.

AS I INDICATED, THE PROPOSED LEGISLATION IS FOCUSED ON "MAINSTREAM" TELECOMMUNICATIONS SERVICE PROVIDERS, ON "COMMON CARRIERS," WHO HISTORICALLY HAVE BEEN SUBJECT TO REGULATION. THIS LEGISLATIVE PROPOSAL SHOULD BE MORE ACCEPTABLE TO THE COMMON

CARRIERS. FOR INSTANCE, THE ELECTRONIC SURVEILLANCE REQUIREMENTS HAVE BEEN CLARIFIED; A NETWORK "SYSTEMS SECURITY" PROVISION ADDED, WHICH SPECIFIES THAT ALL PREMISES-BASED INTERCEPTS (SWITCHES, NETWORK ELEMENTS) MUST BE ACTIVATED EXCLUSIVELY BY COMMON CARRIER PERSONNEL; A MANDATE THAT SUPPORT SERVICE PROVIDERS AND EQUIPMENT MANUFACTURERS, UPON WHOM THE CARRIERS RELY, WILL FURNISH THE TIMELY COOPERATION REQUIRED TO PERMIT COMPLIANCE; AN ATTORNEY GENERAL "CONSULTATION" PROVISION, DESIGNED TO FACILITATE DISCUSSION AND COST-EFFECTIVE APPROACHES TO COMPLIANCE; AND, IMPORTANTLY, FEDERAL GOVERNMENT PAYMENT TO COMMON CARRIERS FOR REASONABLE AND COST-EFFECTIVE CHARGES DIRECTLY ASSOCIATED WITH ATTAINING COMPLIANCE WHICH ARE INCURRED WITHIN THE THREE YEAR PERIOD SET FOR COMPLIANCE.

ALSO INCLUDED IN THE LEGISLATION ARE AMENDMENTS TO THE FEDERAL CRIMINAL ELECTRONIC SURVEILLANCE LAWS ("TITLE III") WHICH IMPROVE COMMUNICATIONS PRIVACY PROTECTION: PRIVACY PROTECTION FOR HANDHELD "CORDLESS" TELEPHONES ON A PAR WITH WIRELINE AND CELLULAR TELEPHONES, CLARIFICATION OF PRIVACY PROTECTION FOR ELECTRONIC COMMUNICATIONS TRANSMITTED BY RADIO, AND PRIVACY PROTECTION FOR COMMUNICATIONS TRANSMITTED USING SECURITY-ENHANCING MODULATION TECHNIQUES.

LAW ENFORCEMENT FULLY SUPPORTS THE INTRODUCTION AND DEPLOYMENT OF ADVANCED TELECOMMUNICATIONS TECHNOLOGIES AS A MEANS OF SHARING INFORMATION, EDUCATING AMERICANS, AND INCREASING OUR PRODUCTIVITY. IN PARTICULAR, WE ARE EXTREMELY SUPPORTIVE OF THE VICE PRESIDENT'S INITIATIVE TO CREATE A NATIONAL INFORMATION INFRASTRUCTURE FOR THE BENEFIT OF ALL AMERICANS. AS WE ALL EMBRACE THE VAST POTENTIAL OFFERED BY ADVANCED TECHNOLOGY, AND ADVANCED TELECOMMUNICATIONS TECHNOLOGY IN PARTICULAR, IT IS CRITICAL THAT THE EQUITIES OF OUR LAW ENFORCEMENT AND INTELLIGENCE AGENCIES NOT BE FORGOTTEN OR IGNORED. HOWEVER, IT WOULD BE WRONG FOR ALL OF US AS PUBLIC SERVANTS, BOTH WITHIN THE EXECUTIVE AND LEGISLATIVE BRANCHES OF GOVERNMENT, TO KNOWINGLY ALLOW THIS INFORMATION SUPERHIGHWAY TO JEOPARDIZE THE SAFETY AND

ECONOMIC WELL-BEING OF LAW-ABIDING AMERICANS BY BECOMING AN EXPRESSWAY AND SAFE HAVEN FOR TERRORISTS, SPIES, DRUG DEALERS, MURDERERS, AND THUGS.

I DO NOT RELISH THE THOUGHT OF BEING THE FIRST FBI DIRECTOR TO TELL A FATHER AND MOTHER THAT WE WERE UNABLE TO SAVE THEIR SON OR DAUGHTER BECAUSE ADVANCED TELECOMMUNICATIONS TECHNOLOGY PRECLUDED THE TELEPHONE COMPANY FROM PROVIDING US WITH LAWFUL ACCESS TO THE CRIMINAL CONVERSATIONS THAT WOULD HAVE PREVENTED THE UNTIMELY DEATH OF AN INNOCENT CHILD. NOR DO I WANT THE PRESIDENT PLACED IN THE POSITION OF HAVING TO TELL THE AMERICAN PUBLIC THAT WE IN LAW ENFORCEMENT COULD NOT PREVENT A VIOLENT TERRORIST ACT DIRECTED AGAINST INNOCENT AMERICANS IN A MAJOR METROPOLITAN AREA SOLELY BECAUSE OF ADVANCED TELECOMMUNICATIONS TECHNOLOGY.

IT IS IMPERATIVE THAT CONGRESS PROMPTLY ENACT THE ADMINISTRATION'S PROPOSED LEGISLATION THAT WILL SOLVE THIS SERIOUS PROBLEM ON A TIMELY AND COMPREHENSIVE BASIS. EVERY DAY THAT PASSES IN WHICH THIS PROBLEM REMAINS UNRESOLVED, THE LONGER THE SAFETY AND ECONOMIC WELL-BEING OF THE AMERICAN PUBLIC ARE UNNECESSARILY PLACED AT RISK. I LOOK FORWARD TO WORKING WITH EACH ONE OF YOU AND THIS CONGRESS REGARDING THE ENACTMENT OF THIS IMPORTANT LEGISLATIVE INITIATIVE.

THANK YOU MR. CHAIRMEN AND THE MEMBERS OF THESE SUBCOMMITTEES FOR PROVIDING ME THIS OPPORTUNITY TO TESTIFY AND PROVIDE YOU WITH INFORMATION CONCERNING THE MOST IMPORTANT PUBLIC SAFETY AND NATIONAL SECURITY ISSUES FACING US TODAY.

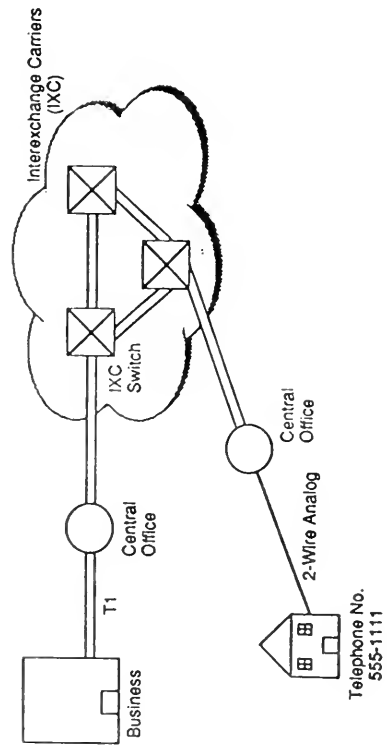
"TITLE III" INTERCEPTIONS¹

Year	Original Interception Applications Authorized			Reported Results	
	State	Federal	Total	Arrests	Convictions ²
1982	448	130	578	2,870	1,886
1983	440	208	648	2,890	2,007
1984	512	289	801	3,719	2,429
1985	541	243	784	4,178	2,616
1986	504	250	754	3,830	2,447
1987	437	236	673	3,225	1,956
1988	445	293	738	3,830	2,404
1989	453	310	763	4,199	2,205
1990	548	324	872	3,167	1,327
1991	500	356	856	2,189	2,185
1992	579	340	919	2,685	607
Total	5,407	2,979	8,386	36,782	22,069

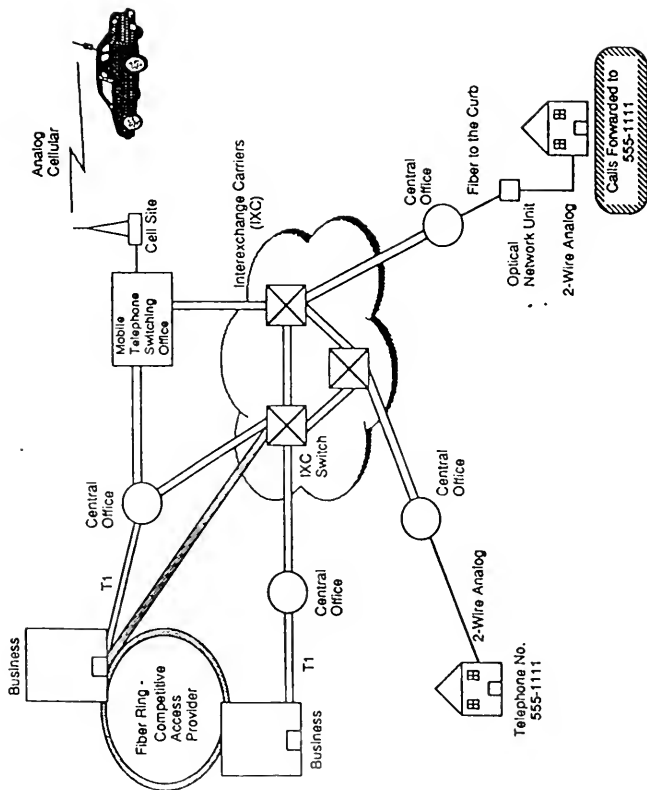
¹ Administrative Office of the United States Courts, REPORT ON APPLICATIONS FOR ORDERS AUTHORIZING OR APPROVING THE INTERCEPTION OF WIRE, ORAL, OR ELECTRONIC COMMUNICATIONS (WIRETAP REPORT) (1983 - 1992).

² A substantial number of prosecutions are ongoing and total convictions will not be reported for several years. Convictions continue to be reported as a result of interceptions going as far back as 1982. Unfortunately, the reporting of convictions appears to lag substantially behind the actual convictions and there are indications that convictions that should be reported by State prosecutors and judges are not actually reported.

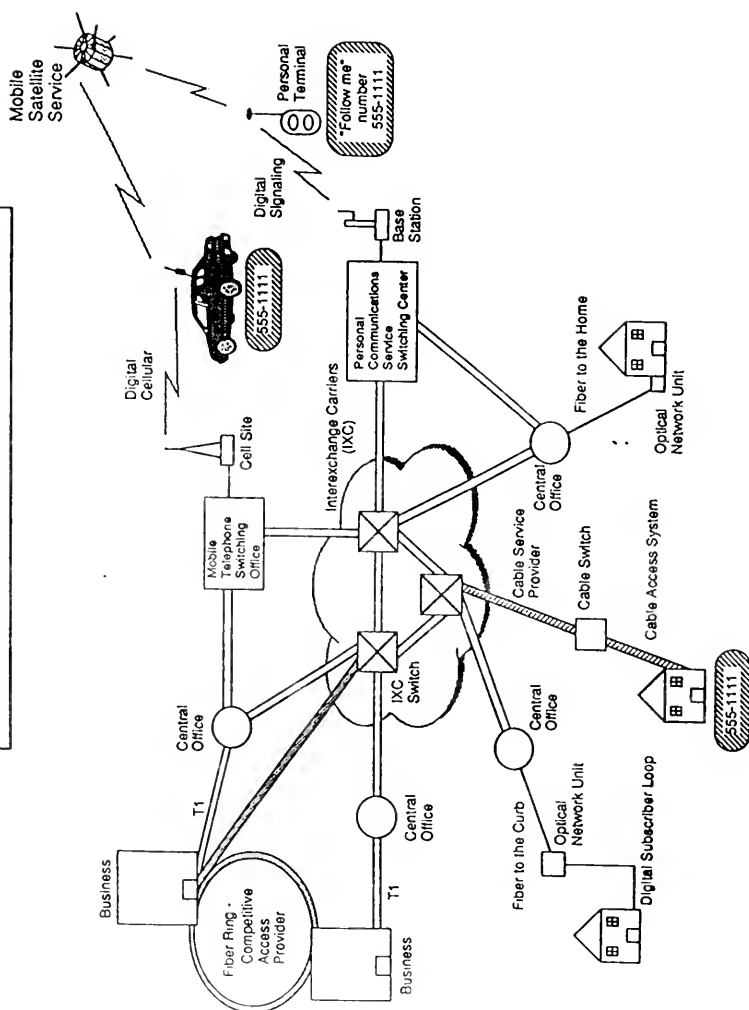
PAST OPERATING ENVIRONMENT



PRESENT OPERATING ENVIRONMENT



FUTURE OPERATING ENVIRONMENT





U.S. Department of Justice

Federal Bureau of Investigation

Washington, D. C. 20535

January 5, 1994

Mr. Casimir S. Skrzypczak
President
NYNEX Science and Technologies, Inc.
120 Bloomingdale Road
White Plains, New York 10605

Dear Mr. Skrzypczak:

Upon receipt of your November 8, 1993, letter, my staff and I conducted a careful and detailed review of the results of the industry working group, which was formed at the request of industry, in March 1992 to address the electronic surveillance requirements of our Nation's state and federal law enforcement agencies. According to senior telecommunications executives, this group was to be "the approach" to address law enforcement's concerns in this area. Although the efforts of industry have been useful to a degree, an honest and candid assessment of the results achieved to date, unfortunately, leads me to conclude that this body does not appear to be equipped or able to develop and implement the solutions that are needed to remove the current and emerging impediments which prevent or hinder law enforcement agencies in executing court orders for electronic surveillance. Although I have held out hope that the industry working group, the Alliance for Telecommunications Industry Solutions (ATIS), and the Electronic Communications Service Providers Committee (ECSPC) would provide a mechanism for achieving solutions and removing the impediments, this recent assessment compels me to acknowledge that these efforts have been inadequate.

As I mentioned in my letter of September 28, 1993, at the outset, back in March 1992, we were pleased with and supportive of the committee's mission to resolve this significant threat to the public safety, national security, and effective law enforcement. To aid in the initiative, we have devoted FBI technical experts and engineers to this process, as well as funding a telecommunications consulting firm to facilitate meetings, provide subject matter expertise, and prepare written contributions. Also, as I previously mentioned, some of the industry representatives have worked hard and appear to have been sincere in their efforts to reach solutions. However, some companies have not supported these efforts and others have not contributed meaningfully to the effort. In my estimation, this is a result of the voluntary basis and elective nature of the working group and committee approach. Particularly troubling is the fact that new service providers who are now entering the marketplace are unaware of law enforcement's requirements, and efforts by the FBI to have these requirements brought to the attention of industry standards bodies, such as the one now considering Personal Communications Services (PCS) systems, were not supported by industry representatives in the committee.

I believe that in order to successfully accommodate law enforcement's needs and to ensure that electronic surveillance responsibilities are discharged as new technologies emerge, a mechanism must exist that, in a certain and comprehensive fashion:

- Identifies fully law enforcement's electronic surveillance requirements to the telecommunications industry;
- Prompts the technical solutions necessary to meet the requirements of law enforcement;
- Assures timely implementation of these solutions into the telecommunications industry's existing and emerging technologies; and
- Addresses the cost issues associated with the technical solutions and their implementation.

Time has shown that the ECSPC, by itself, is not capable of achieving our goal of ensuring the ability of law enforcement to perform electronic surveillance without fail within existing and emerging telecommunications systems.

As I have previously indicated, the efforts of many committee members have been greatly appreciated by law enforcement. However, it is apparent that the recommended industry approach, the ECSPC, cannot address all of the necessary elements I have listed above. In fact, several committee members have made the point that, as matters stand, only an individual company can determine whether or not it is willing to pursue and implement solutions once they are identified.

It is my view that the committee process should be a mechanism for discussing law enforcement needs and identifying technical solutions. Committee products thus far, such as those reflected in the ISDN, Digital Loop Carriers, and Cellular action teams' written recommendations, have not included solutions, but rather have largely only restated law enforcement's current abilities and limitations in performing electronic surveillance in these technical environments--information which the FBI itself provided nearly two years ago. In the main, these products observe the need for the development of solutions to meet law enforcement needs, but they do not provide these solutions. Inasmuch as the committee is not empowered to resolve cost and other issues key to the implementation of solutions, the lack of meaningful and timely solutions to these technological problems will continue.

As we have indicated previously, we shall continue our active participation in the committee process. However, given the results to date, we are also obligated to pursue other approaches which will ensure law enforcement's continued ability to protect the safety and economic well-being of the American public through the use of this essential investigative technique.

Sincerely yours,

James K. Kallstrom
Special Agent in Charge



nce for Telecommunications
Industry Solutions
Exchange Carriers Standards Association

March 1, 1994

Problem Solvers to the
Telecommunications Industry

1000 G Street, NW
Suite 500
Washington DC 20005

202-545-6380
Fax: 202-353-5452

Casimir S. Skrzypczak
Chairman
AT&T Corporation

Frank D. Kress
Vice Chairman
North Pittsburgh Systems, Inc.

Gregory L. Thain
Treasurer
GTE Telephone Operations

George L. Edwards
President
ATIS

Susan M. Miller
Secretary & General Counsel
ATIS

Committees

Committee 1:
Telecommunications

Common Law Committee

Information Industry
Privacy Forum

Information Industry
Lawyer Committee

Protection Engineers Group

Standards Committee 01

Electronic Communications
Service Providers Committee

Electronic Communications
Service Providers Committee

Electronic Communications
Service Providers Committee

Mr. James K. Kallstrom
Special Agent in Charge, Special Operations Division
Federal Bureau of Investigation
26 Federal Plaza
New York, NY 10278

Dear Jim,

I am writing in response to your letter of January 5, 1994, in which you expressed your concerns regarding industry efforts to address the electronic surveillance requirements of state and federal law enforcement agencies.

First, let me say that your observations regarding the functioning of the Electronic Communications Service Provider Committee (ECSP) and its progress to date in resolving issues are understandable. These comments included: the Committee is not equipped to implement the technical solutions which it identifies; some companies have not supported these efforts and others have not contributed meaningfully to the effort; and, efforts by the FBI to have law enforcement's requirements brought to the attention of industry standards bodies were not supported by all representatives on the Committee. However, these observations which you find troubling are aspects of the committee process which are fundamental to the operation and interest of open industry forums.

One of the basic principles of any inter-industry committee or forum is that solutions reached are proposals for voluntary implementation by the participants; recommendations are non-binding. While each participant is committed to good faith discussions and consideration of timely implementation, each company represented also reserves fully independent judgment in terms of any implementation. This tenet of operation serves a number of purposes, a key one being that it mitigates the legal/antitrust risks of conducting these discussions in any industry meeting.

Mr. James K. Kallstrom
 Page 2
 March 1, 1994

The forum process also ensures that there is careful consideration of all views and objections, appropriate notification and opportunity for the industry to review and provide comments on any proposed solution, and ultimate resolution by consensus. While there is no guarantee, the fact that all participants have been a part of these sensitive discussions, have been afforded due process, and have willingly expended the necessary resources in the development of a solution, more often than not results in strong incentives to implement. It simply may not produce the direct and open commitment to implement solutions at the Committee level that you appear to be looking for.

As I am sure you are aware, most of the solutions developed or being discussed are costly to implement, and can require months, even years to develop. Quite frankly, decisions of this magnitude require review by higher levels of management than those representatives present at the ECSP Committee. Industry sends the subject matter experts to these meetings to develop the technical solutions. Typically, industry does not send representatives who are authorized to make business decisions which may involve large expenditures. While you may view that as a shortcoming of this industry process, I believe that federal agencies operate in the same fashion.

Another characteristic of industry forums is that participating companies do not support and/or contribute to efforts equally. Participants tend to gravitate toward and contribute to those issues in which they have the most interest or the greatest business need. They rely on other participants to provide leadership on the remaining issues. Over time, leadership and contributions tend to balance. Evaluating an individual company's commitment to the process by its level of participation on a single issue can possibly provide a distorted view. The fact that a particular company is not among the leaders on a particular issue does not mean it is not aware or does not care about what is being discussed. The minutes or notes of all meetings, as well as the contributions discussed, are available to all participants for review and comment; and I assure you they are scrupulously reviewed. The stakes are simply too high for them to be ignored. Even though resolutions and recommendations are non-binding, no company wishes to be part of a consensus it cannot ultimately support.

Your concern that efforts by the FBI to have law enforcement's requirements brought to the attention of industry standards bodies were not supported by all industry representatives on the Committee, has proved short lived. At the October meeting the Committee agreed to provide a contribution to the Joint Experts Meeting (JEM) on Privacy and Authentication for Personal Communications held November 8-12. It was reported at the December 1993 Committee meeting that at the JEM the law enforcement requirements were presented and

Mr. James K. Kalstrom
 Page 3
 March 1, 1994

discussed. The Committee observed that the "objective to raise awareness of the needs of law enforcement to support surveillance were met." At the most recent meeting of the ECSP Committee, the PCS action team was empowered by the full committee to prepare and submit contributions to a number of standards bodies addressing PCS issues. The initial reluctance of the Committee to support this effort was no doubt due to the short turn-arounds required to prepare and approve contributions, and the fact that both industry and law enforcement continue to insist that nearly all Committee documents be considered proprietary. The standards process is an open, public process which requires that all contributions submitted be non-proprietary. Similarly, if new service providers are to become aware of law enforcement's requirements, those requirements must be publicly available. To date, the Committee has been reluctant to publicize these requirements in the belief that to do so will serve to highlight current shortcomings.

Even though discussions between law enforcement and industry have been ongoing for some time, this particular committee, which is co-chaired by industry and law enforcement, and its incumbent operating principles, has been in existence for less than one year. Participants are only now gaining the mutual respect required to bring forth meaningful solutions. You note the fact that the Committee's products to date merely "observe the need for the development of solutions to meet law enforcement needs." I see this as a necessary step forward. If meaningful solutions are to result, all participants must first understand that there is in fact a problem, not that one participant, or one group of participants, says so. Now that the Committee recognizes the problems, it can proceed to identify and develop appropriate solutions.

I understand your obligation to pursue whatever approaches you deem necessary to ensure law enforcement's continued ability to conduct the lawful intercept of communications. However, whatever those other approaches may be, and whatever results those approaches may yield, it will still be necessary for industry and law enforcement to work together to identify and develop suitable technical solutions. I believe the ECSP Committee is the appropriate forum for that purpose.

Sincerely,

Casimir S. Skrzypczak
 ATIS Chairman

Organized Crime Appendix

The President's Commission on Organized Crime stated the following conclusions in its report, The Edge: Organized Crime, Business and Labor Unions:

- If unchecked, organized crime can take over, own, and operate legitimate business. It can also control entire industries. The ways in which industry can be affected are by the increased price of items due to theft, bribery (kick-backs), price fixing and the control of trade.
- The control of the marketplace by organized crime is also obtained by the control of unions and by monopolizing power in specific industries.
- Through the control of unions, payoffs can be demanded to ensure labor peace. Businesses comply with the labor union's demands rather than lose profits or lose business. Another deleterious effect of organized crime control is through the illegal utilization of union funds. At the time of the report of the PCOC, union benefit funds had cumulative assets of over \$51 billion. Influence in the unions on a local level, if strong enough, may lead to control of the union at the international level.
- The costs of labor racketeering are hard to trace. The Commission estimated that millions of dollars in workers' labor union dues were stolen from the unions through embezzlement, lost through illegal loans, and taken through extortionate and illegal fees paid to trust and service fund providers.

As a result, the U.S. public is forced to pay higher commodity costs because of organized crime's control. Examples cited by the Commission of the various types of economic loss are:

- Amalgamated Local 355, an independent union in Queens, New-York, lost nearly \$2 million in a kickback and embezzlement scheme in the mid-1970s. The scheme involved the union's secretary/treasurer and a well-known real estate developer.
- The control of the concrete industry by the LCN in New York, as brought out in the LCN Commission indictment, was demonstrated in evidence which showed that over the period 1981 - 1984, the 2% skim collected on the total cost of poured concrete, on the delivery of it to the job site, and on the attendant labor costs could range anywhere from \$1.6 to \$3.5 million. This figure was estimated on the control of the concrete industry alone. Increased construction costs then lead to higher overall building project costs and increased rental rates, etc. Essential evidence supporting this prosecution was derived from electronic surveillance.

Through the utilization of electronic surveillance, Federal and state investigations continue to have a significant impact upon organized crime groups. In Fiscal Year 1991, at the Federal level, there were 239 recorded convictions and 246 indictments of LCN members and associates. In addition, civil RICO complaints spawned by the criminal investigations were filed against 25 individuals and/or entities, and judgments were entered against 23. Aggressive use of the seizure and forfeiture provisions of the RICO statute yielded \$17,554,865. Over \$11,779,106 in fines were levied against convicted individuals; recoveries and restitutions totaling \$22,881,539 were obtained; and \$7,044,625 in potential economic losses were prevented. A few recent cases, wherein electronic surveillance played a critical role, illustrate the importance of maintaining the efficiency of this investigative technique.

- Commercial seafood and longshoremen dock-loading industries. For over 70 years, organized crime, and particularly the Genovese LCN family, had dominated and controlled the Fulton Fish Market and its immediate environment in New York City. Through electronic surveillance which spanned over two years, the government acquired substantial evidence as to the influence and control of organized crime in the seafood industry and the labor unions related to it. As a result, in October 1987, a civil RICO complaint was filed against the Genovese LCN crime family, certain unions controlled by organized crime, and a number of LCN members and associates. In 1988, in a landmark RICO decree and judgment, the Fulton Fish Market was placed under the oversight of a court-appointed administrator. Judgments in this civil RICO action permanently bar the Genovese LCN crime family and other defendants from having any future dealings in that seafood market.

Although it is difficult to quantify the impact of the government's intervention into this industry, the enormous economic and social costs associated with the LCN's control of this market have been significantly reduced. Illegal activities such as hijacking, gambling, robbery, burglary, loansharking, extortion, murder, narcotics trafficking, and labor racketeering flourished in the Market's environment while under the dominion of the LCN. These activities have dramatically abated with the imposition of the consent and default judgments. The court-appointed administrator and other independent sources of information, such as the media, report that the Fulton Fish Market has sales approximating two billion dollars annually. Seafood that passes through the market is bought and sold throughout the United States. Illegal activity at the Market has inflated seafood costs by \$1 - \$2 dollars per pound and virtually every household in America has absorbed that cost. By a conservative estimate, the American public has been spared literally millions of dollars in increased seafood costs as a result of this investigation.

- International Longshoremen's Association. This investigation focused primarily upon corruption on the New York and New Jersey waterfront, the second largest port in the world. The civil RICO complaint names as defendants the International Longshoremen's Association (ILA), their executive

boards, six local labor unions, and 32 present or former officials of these ILA locals, 21 of whom are identified as members or associates of the Gambino and Genovese LCN crime families, and the "Westies" criminal gang. Twelve additional individuals are identified in the complaint as members or associates of the Gambino and Genovese LCN families and the Westies, and several employers in industries affecting waterfront commerce are named for purposes of obtaining adequate relief.

The complaint alleges that the LCN figures have used these locals and their various affiliated benefit funds to conduct a pattern of racketeering activity on the waterfront, which includes murder, extortion, embezzlement of union funds, illegal labor and benefit fund payments and mail fraud. To prove such wide-ranging conspiracies, the type of evidence needed typically requires substantial reliance upon electronic surveillance-based information.

These investigations, which heavily relied upon electronic surveillance, demonstrated an extraordinary breadth of control by the Genovese LCN family over waterfront activity that extended from the New York - New Jersey piers all the way to the Port of Miami. This pervasive control by organized crime over the waterfront extends back to the turn of the century. Organized crime obtained this control by its early recognition that to transport goods to the eastern seaboard, markets often required passage through the New York/New Jersey waterfront, and that this transportation terminal point presented a labor intensive bottleneck. To control waterfront labor, thus, was to exercise tremendous leverage over the entire shipping industry, effect the commerce of a huge section of the American economy, and ultimately to drive up prices of a myriad of commodities sold in the United States.

There are numerous other examples where, through the use of court-ordered electronic surveillance, major economic harm was abated. The nationwide investigation into organized crime-labor racketeering influence in the union health and dental care industry has resulted in the termination of frauds and kickbacks which cost unions and insurance companies millions of dollars. In one investigation, sixteen different FBI field offices were involved, eight of which conducted extensive electronic surveillance. At the conclusion of the investigation in September, 1988, seven separate Federal Grand Jury indictments were returned in Atlanta, Chicago, Baltimore, San Diego, and San Francisco, charging ten individuals and five corporations with numerous Federal violations including RICO, conspiracy, mail fraud, wire fraud, and labor racketeering. As a result of this investigation, ten health care executives were convicted, the U.S. Public Health Service changed its bidding procedures nationwide, SAFECO Insurance Company terminated its practice of paying double commissions to insurance agents nationwide, and spin-off investigations resulted in the conviction of a Federal judge and two labor-related, organized crime leaders.

Electronic surveillance was extensively utilized in the landmark civil RICO investigation called "Liberatus" which resulted in the formal break up of LCN control over the nation's largest union, the International Brotherhood of Teamsters. The LCN's grip over this union had been intact since the 1950s. As a result, for the first time in decades the nation's largest union is free from organized crime control and corruption, and the continued pillage of union funds has ceased.

Mr. FREEH. On March 25, the administration formally transmitted to Congress a legislative proposal to address this critical law enforcement issue. The legislation that subsequently evolved was introduced in both Houses of Congress on August 9 by Chairman Edwards and Chairman Leahy. This proposal offers strong assurance that this critical investigative technique will be preserved while ensuring that the privacy of law-abiding citizens remains protected and that the telecommunications industry remains fully competitive, both at home and abroad.

Court-authorized electronic surveillance is clearly one of law enforcement's most important and effective investigative techniques. It is often the only way to prevent or solve some of our most serious crimes. However, law enforcement's ability to conduct such court-authorized surveillance is directly threatened because of advances in telecommunications networks and the deployment of new digitally based technologies. Industry representatives acknowledge that some existing networks and planned future networks prevent carriers from being able to comply fully with such orders and prevent giving law enforcement access to all communications and dialing information within such court orders.

Technological impediments to electronic surveillance indeed exist. Federal legislation is the only realistic solution. The evidence with respect to the existence of this problem is, in my view now, a consensus agreement by all of the parties who have been discussing this. The recently completed GAO study, which this committee has been furnished, clearly recognizes the problem, both in current and future technologies.

Second, for 2 years an industry technical working group has been specifically tasked and working to solve the realistic problem.

Third, an informal FBI survey last year found 183 separate incidents around the country where Federal, State or local law enforcement wiretap efforts were frustrated.

Fourth, USTA President Roy Neel acknowledged during congressional testimony on August 11 that new, enhanced telecommunications technology is hampering and will continue to hamper law enforcement's wiretapping efforts.

H.R. 4922 carefully balances the legitimate concerns of law enforcement, the telecommunications industry and privacy advocates by addressing the public safety concerns and yet affording great privacy protection to telephone users and ensuring fair and equitable treatment for carriers. The bill reflects reasonableness throughout its provisions. The legislation focuses on common carriers, entities that historically have been subject to regulation.

It is within those networks that almost all the problems have occurred and will continue to occur in the foreseeable future. Thus, small, private, branch PBX operators, pure computer networks and private networks need not alter their systems and networks. Even within common carrier networks, carrier responsibilities are removed or limited in such key areas as communication links exclusively dedicated to interconnecting carriers and private networks. Cellular carriers need not artificially reroute communications and are only required by the legislation to notify law enforcement of the identity of a new cellular carrier when a cellular call hand-off occurs. Information services are excluded.

As a further accommodation to industry, we agreed to language which extends the compliance period from 3 to 4 years with an extension provision of up to 2 additional years where good faith and reasonable efforts require it. We also agreed to language that explicitly states that law enforcement may not dictate or require the specific design or features of system configurations. Nor may law enforcement prohibit the adoption of any feature or service. Law enforcement has no intention of becoming a technologies czar or regulating development of new beneficial telecommunications systems, services or features.

In response to industry concerns, the legislation requires the Attorney General to specify a capacity requirement in the first year after legislative enactment. This will furnish carriers with our short-term and longer-range capacity requirements so that capacity will not be needlessly undersized or oversized.

Under the legislation, carriers may rely on industry-based technical requirements and standards meeting law enforcement requirements, a so-called "safe harbor", thereby preventing needless concern about civil liability. Further, any dispute regarding technical requirements or standards may be brought to the FCC for resolution.

We have agreed to language that precludes enforcement orders against carriers where alternative technologies or technical capabilities exist or where the law enforcement requirements were better met by another carrier. Such orders would not issue where compliance is not reasonably achievable through available technology. In any case, before a court could assess a civil penalty, it must consider the nature, circumstances and extent of the violation and the carrier's ability to pay, good-faith efforts to comply, and any effect on its ability to continue to do business.

We all recognize, as several members have pointed out, that cost has to be addressed. Payment to carriers is desirable if we are to address industry's concerns and still maintain effective law enforcement and ensure public safety. The administration's proposal and H.R. 4922 both require the government to reimburse carriers for making the necessary modifications to existing systems to achieve compliance during the specified compliance period, with industry being responsible thereafter for costs associated with compliance concerning future systems and features.

In addressing other public welfare and safety issues, industries and businesses have frequently been required to install sprinkler systems, smoke detectors, fire alarms, fire escapes, safety belts, air bags without the benefit of government funding. As you recall, within the communications industry, in 1990, Congress mandated that televisions include closed-captioning technology for the hearing impaired without government reimbursement. At that time, industry representatives exaggerated the possible negative effects of the legislation, claiming that this requirement would substantially increase the cost of future televisions.

In fact, the actual cost per television was about one-quarter of the cost estimated by the industry. Nonetheless, I believe government funding is important in assisting the telecommunications industry to meet its existing legal responsibilities under the technical

assistance requirement placed on carriers by Congress nearly 25 years ago.

In any case, the cost to remove this threat to public safety and national security pale in comparison to the devastating loss of life and economic impact if law enforcement's wiretapping efforts continue to be hampered by technological impediments. One need only be reminded of the magnitude of the crimes facing society today and as we go into the 21st century, for example, the terrorist bombing in New York City of the World Trade Center resulting in the loss of 6 lives, over 1,000 injured persons and an economic cost of over \$5 billion as estimated by the New York Port Authority. Or the cost of the FBI's prevention of a second similar occurrence in New York City. Or the FBI's prevention of a planned rocket attack against a commercial airliner by a terrorist group in Chicago.

If saving lives is important, I believe any cost-benefit analysis comes down on the side of protecting public safety.

What does an FBI agent or an FBI Director or a Congress say to the father of Polly Klaas when we know that the technique that is at stake here could be involved and used in saving a particular child? We can't put costs on the lives of people, children and the people that we are all sworn to protect.

On a cost-benefit analysis, if you figure that the total combined Federal, State and local wiretaps in any calendar year are under 1,000, you would say by most economic means that the technique was not worth the money being spent. If you factor into that the cost of the resources put into these cases, any reasonable cost-benefit analysis would argue against wiretapping. No one would dare make such an argument because what is at stake here are the lives of people and the children we are sworn to protect.

The concerns of privacy advocates are well addressed in the legislation. Numerous provisions extend privacy protection and ensure network security. For example, all electronic surveillance efforts initiated in switching premises must be activated only by carrier personnel. Privacy protection is balanced regarding government access to interactive transactional records.

Law enforcement is required to utilize pen register technology, when reasonably available, that captures only dialing or signaling information used in call processing. Also precluded is any location information incidental to the execution of pen register court orders or subpoenas. Privacy protection is conferred on the radio portion of cordless telephone communications.

After numerous meetings and drafting sessions with congressional staff, carrier and privacy representatives, balanced legislation has now been crafted. The overriding public safety considerations demand that a legislative solution be found quickly. Everyone has made concessions and acceptable compromises in light of competing concerns and considerations.

Once again I would like to thank you, Chairman Markey, and members of the subcommittee, for holding this hearing; and I encourage your collective support for enactment of H.R. 4922 during this session of Congress. This is a drop-dead issue for law enforcement, and I by no means confine that to the FBI or Federal law enforcement.

As you know, the State and local prosecutors and police forces around the country conduct the majority of wiretaps in this country. It is the view of the FBI and the Department of Justice, the administration and my colleagues represented here with me today from local law enforcement that this is an issue which begs the attention and the immediate concern not only of all Americans but this Congress and this very distinguished committee.

Thank you very much, sir.

Mr. MARKEY. Thank you very much.

[The prepared statement of Louis J. Freeh follows:]

STATEMENT OF LOUIS J. FREEH, DIRECTOR, FEDERAL BUREAU OF INVESTIGATION

Mr. Chairman, let me thank you for providing me this opportunity to discuss with you one of the most important issues facing law enforcement today—the grave threat of our continued ability to conduct court-authorized electronic surveillance, also known as the “digital telephony issue.”

On March 18, 1994, I appeared before a joint hearing of House and Senate Judiciary Subcommittees chaired by Congressman Edwards and Senator Leahy. At that time I provided a detailed statement for the record explaining the tremendous importance of court-authorized electronic surveillance to law enforcement. My statement also discussed the technological impediments that impact on such surveillance, and the dire consequences to effective law enforcement, the public safety, and the national security if no binding solution to this problem is obtained. With your permission, Mr. Chairman, I would like to provide a copy of that statement to the subcommittee for your information.

On March 25, 1994, the administration formally transmitted to the Congress a legislative proposal to address this critical law enforcement issue. I believe that the legislation that has subsequently evolved, and that was introduced in both Houses of Congress on August 9th by Congressman Edwards and Senator Leahy (H.R. 4922 and S. 2375), offers strong assurance that this important investigative technique will be preserved while at the same time ensuring that the privacy of law abiding telephone users remains protected and that the telecommunications industry remains fully competitive, both domestically and internationally.

As I have previously indicated, court authorized electronic surveillance is one of law enforcement's most important and effective investigative techniques and is often the only way to prevent or solve some of the most serious crimes facing today's society. However, because of advances in telecommunications networks, the introduction and deployment of new digitally-based technologies, services and features, law enforcement's ability to conduct court authorized surveillance is being threatened. Industry representatives have acknowledged that existing networks and networks planned for the future prevent common carriers from being able to fully comply with court orders and provide law enforcement with access to all communications and dialing information set forth in the orders.

I believe that we have clearly demonstrated that technological impediments to electronic surveillance indeed exist, that Federal legislation is the only realistic solution, and, as I indicated on March 18th, that from the outset we have been willing to accommodate every reasonable concern raised by the telecommunications industry and privacy advocates. Over the past decade, we estimate that several hundred court orders have been frustrated, either in part or in whole, by various technological impediments but some still question the need for legislation, saying there are no problems. However, evidence to the contrary is overwhelming. First, a recently completed General Accounting Office study documented technological impediments to wiretapping in current and future technologies. Second, the existence for over 2 years of a technical working group of telecommunications industry representatives and law enforcement, created specifically to examine possible solutions to such technological impediments, clearly demonstrates the existence of real technical problems. Third, an informal survey conducted by the FBI, and updated this spring, identified 183 incidents where Federal, State, or local law enforcement wiretap efforts were frustrated, and investigations hampered, by such technological impediments, thus threatening public safety. Lastly, the recent acknowledgement by United States Telephone Association president Roy Neel during congressional testimony on August 11th that new, enhanced telecommunications technology is hampering and will continue to hamper law enforcement's wiretapping efforts dispels any doubt about the reality of this problem.

It is my view that H.R. 4922 carefully balances the legitimate concerns of law enforcement, the telecommunications industry, and privacy advocates. It is the product of intense discussion, give and take, and compromise by all parties involved. The FBI, privacy and industry representatives, and congressional members and staff have worked extremely hard, and I believe, have been flexible, in order to reach a satisfactory legislative solution which addresses the public safety concerns of the law enforcement community and yet affords great privacy protection to telephone users and ensures fair and equitable treatment for telecommunications carriers.

The hallmark of H.R. 4922 is reasonableness. The language of the legislation reflects reasonableness in every provision. For example, the coverage of the legislation focuses on common carriers—entities that historically have been subject to regulation. We have acknowledged that almost all of our electronic surveillance problems have occurred, and will continue to occur in the foreseeable future, in the networks and systems of common carriers. Therefore, this legislation does not unreasonably and unnecessarily call upon small private branch exchange (PBX) operators, pure computer networks. Even within common carrier networks, we have agreed to language which reasonably limits carrier responsibilities in certain key areas. The legislation does not require common carriers to satisfy the electronic surveillance requirements by assuring access to targeted communications where the communications link is one that exclusively is dedicated to interconnecting carriers and private networks. Second, information services are excluded. And third, with regard to cellular communications that are handed off to other common carriers or to other service areas, we have agreed to language which specifies that the initial carrier need not artificially reroute communications, and we have settled upon being advised as to the identity of the new carrier when such a hand-off occurs.

Because some carriers have expressed a concern about meeting these requirements within 3 years, as originally proposed by the administration, we have agreed to language which extends this period to 4 years, and which also permits a carrier to request an extension or extensions of up to a total of 2 more years where the carrier can show that good faith and reasonable efforts require more than the 4-year period.

We have also agreed to language which explicitly states that law enforcement may not dictate or require the specific design of features or system configurations. Nor may law enforcement prohibit the adoption of any feature or service. As I have said on numerous occasions, law enforcement has no intention of becoming a technology czar or of regulating the development of new and beneficial telecommunications systems, services or features.

Because telecommunications industry representatives have expressed a concern that the administration's proposal did not specifically address the capacity requirements that would be placed on each carrier, we developed, and the legislation includes, provisions which clearly place an affirmative responsibility on the attorney general to advise carriers of law enforcement's specific capacity requirements within the first year after enactment of the legislation. These provisions will furnish carriers both with our short-term needs and our longer range capacity requirements, such that the required capacity will not be needlessly undersized or oversized.

We have agreed to language regarding carrier reliance upon industry-based technical requirements and standards that meet law enforcement's requirements which serve as a so-called "safe harbor" for carriers and prevent needless concern about civil liability exposure where good faith efforts are made to comply with such technical requirements or standards. Further, in case of any dispute with regard to such technical requirements or standards, any person may petition the FCC to institute proceedings to resolve any conflict and establish appropriate requirements or standards consistent with the electronic surveillance requirements set forth in the legislation.

With regard to enforcement, we have agreed to language that allows a carrier to prevent the issuance of an enforcing court order under circumstances where alternative technologies or technical capabilities exist or where the law enforcement requirements are better met by another carrier. Further, such an order would be precluded where compliance is not reasonably achievable through the application of available technology and timely action has been taken. Finally, an enforcement action is flatly precluded where the capacity demands exceed those for which the carrier has been provided notice. In any case, before a court can assess a civil penalty it would be required to take into account the nature, circumstances, and extent of the violation, and, with respect to the violator, ability to pay, good faith efforts to comply in a timely manner, effect on ability to continue to do business, the degree of culpability or delay in undertaking efforts to comply, and other matters.

Perhaps of greatest concern to the telecommunications industry is the issue of cost. We all recognize this is a highly competitive industry and that the issue of cost

had to be addressed to make this solution practical. The administration's proposal and H.R. 4922 both require the government to reimburse carriers for making the necessary modifications to existing systems to achieve compliance during the specified compliance period, with industry being responsible thereafter for costs associated with compliance concerning future systems and features. In my view, payment to carriers is desirable if we are to meet the concerns of industry and still maintain effective law enforcement, ensure the public safety, and protect national security. For other public welfare and safety issues, such as the installation of sprinkler systems, smoke detectors, fire alarms, fire escapes, safety belts, and air bags, to name but a few, industry has been required to fulfill these obligations without benefit of government funding. I believe that government funding should be viewed as a substantial effort to assist industry in meeting the "technical assistance" requirement placed on carriers by Congress some 25 years ago. In any case, the costs incurred to remove this threat to public safety and national security pale in comparison to the devastating economic impact, as well as the loss of life, if law enforcement's wiretapping efforts continue to be hampered by technological impediments.

We have also been very willing to address the concerns of privacy advocates, which the provisions of the legislation make clear. First of all, there is the basic requirement that carriers fulfill their electronic surveillance assistance requirements in a manner that protects the privacy and security of communications and information of all subscribers whose communications are not authorized to be intercepted. Second, there are systems security provisions which enhance privacy and security by requiring that all electronic surveillance efforts initiated in switching premises be activated only with the affirmative intervention of a carrier employee. Third, enhanced privacy protection is included with regard to governmental access to any interactive transactions for which a carrier may keep a record. Fourth, law enforcement is required to utilize pen register technology, when reasonably available, that restricts the recording or decoding of electronic or other impulses to the dialing or signaling information utilized in call processing. Fifth, the assistance requirements in these bills exempt the provision of any location information associated with the use of cellular or mobile communications incidental to the execution of pen register court orders or pursuant to a subpoena. Finally, there are a number of privacy enhancing amendments to the electronic communications privacy Act of 1986, the foremost of which is the conferring of privacy protection on the radio portion of cordless telephone communications.

After numerous meetings and drafting sessions with congressional staff, telecommunications industry representatives, and privacy advocates, balanced legislative language has been developed that, I believe, is acceptable to the affected parties. We all recognize that this issue is a difficult one, one which each of the parties approaches from a distinctly different vantage point. All parties have worked hard and all have been flexible. It is understandable that a small number may not be enthusiastic or strong advocates for legislation. However, public safety demands that a legislative solution be found and found quickly. I believe that this is why everyone has made concessions and reached acceptable compromises. I also believe that this is why all acknowledge that the legislation is reasonable and acceptable as a means of resolving this critical law enforcement problem in light of the competing concerns and considerations.

Once again, I would like to personally thank you, Chairman Markey, and members of the subcommittee for holding a hearing on this difficult issue and I encourage your support for the enactment of H.R. 4922 during this session of Congress to resolve this critical problem. This is a "drop dead" issue for law enforcement. Passage of H.R. 4922 will ensure law enforcement's continued ability to protect the American public and safeguard our national security through the use of this vital investigative technique, while being ever mindful of legitimate privacy and industry concerns.

At this time I would welcome any questions you may have.

Mr. MARKEY. And now we will hear from our second witness, Hon. Thomas Reilly, who is district attorney for Middlesex County in Massachusetts. He is here representing the National Association of District Attorneys, and he is nationally recognized as one of the most respected district attorneys in the United States.

We welcome you before us today, Mr. Reilly. Whenever you are comfortable, please begin.

STATEMENT OF THOMAS REILLY

Mr. REILLY. Thank you, Congressman Markey and the members of this committee, for the opportunity to speak in support of the need for Federal legislation to assure that Federal, State and local law enforcement agencies retain the capability to perform court-authorized electronic surveillance in light of emerging digital technologies.

I am Tom Reilly, district attorney for Middlesex County, Massachusetts, and I represent the law enforcement interests of the million-and-a-half people who live in the urban, suburban and rural areas of that county. I am also proud to serve today as a representative of the National District Attorney's Association to provide you with the views of that 7,000-member organization.

In July of this year, our board of directors representing all 50 States unanimously passed a resolution supporting the need for this legislation. Court-authorized electronic surveillance is one of the most important and effective tools that State and local prosecutors have to fight and to prevent crime. Often, it is the only tool. In the past several years in Middlesex County alone, court-ordered electronic surveillance has led to successful investigations and convictions of drug traffickers who poison our youth.

In a series of wiretaps targeting extortion, loan sharking, and money laundering, we have been successful working within the FBI in penetrating the very highest levels of organized crime operating in Massachusetts and New England. Electronic surveillance has also been used by us to prevent the escape from prison of a convicted murderer. These examples are but a few of the examples of the vital importance of electronic surveillance to State and local prosecutors who conduct well over 50 percent of all court-authorized wiretaps across this country.

I want to emphasize to you that electronic surveillance is a sophisticated, complicated operation which is not entered into lightly by law enforcement. In addition to the requirement of a court order based upon probable cause, most States require further administrative requirements to preclude abuse of this surveillance, and there is frequently, as in Massachusetts, a requirement to make periodic reports to the court on the progress of the surveillance.

There is also a significant financial and manpower requirement on the agency conducting the surveillance. Further, the telecommunications industry serves as part of the protective balance. I can assure you that local law enforcement does not have the capability to directly intercept telephonic communications and that the industry will not provide the requested technical assistance in the absence of a court order.

I am here today to alert you to the fact that unless Congress intervenes legislatively, this vital and effective tool will be taken away from law enforcement and threaten public safety throughout this country. The problem is caused by advancing telephone technology which is making it increasingly difficult, if not impossible, to preserve the essential essence of electronic surveillance: The ability to identify, segregate, and provide access to specific calls of criminals who are the subject of court-authorized electronic surveillance.

Without this capability, court-approved electronic surveillance will soon become a thing of the past to the benefit of criminals who victimize us, and who have access and do not hesitate to use the latest technology.

While we as prosecutors welcome technological advancement and realize that the negative impact on law enforcement and public safety is unintentional, we believe a legislative solution is necessary. We urge you to act now. We support the administration's "Digital Telephony Act of 1994", introduced by Congressman Edwards. This legislation simply requires telephone companies, when served with a court order, to continue to assist law enforcement, as they have for the past 50 years, by having the capability to identify, segregate, and provide access to the conversations of specific criminals and target numbers, to the exclusion of all others, regardless of the technology, services, or features involved.

As prosecutors, we simply ask that our scientists and engineers put their unlimited talents to work in assuring that law enforcement is not left blindfolded. We support this legislative solution because it requires the telecommunications industry to meet the needs of law enforcement, but it allows the industry to decide the most efficient and effective approach.

The debate about the need for electronic surveillance has already taken place. The Congress and most State legislative bodies have resolved that in certain cases, and only as a last resort, law enforcement may seek an impartial court order to perform limited electronic surveillance. We as prosecutors fully support this cautious, restrictive approach. Through this legislation, we seek nothing more than to preserve the capability that you and State legislators throughout this country have already authorized in what is a vital tool in our fight against crime.

Thank you.

[The prepared statement of Thomas Reilly follows:]

STATEMENT OF THOMAS REILLY, DISTRICT ATTORNEY, MIDDLESEX COUNTY,
MASSACHUSETTS

Thank you for the opportunity to speak in support of the need for Federal legislation to assure that Federal, State and local law enforcement agencies retain the capability to perform court authorized electronic surveillance, in light of emerging digital technologies.

I am Tom Reilly, District Attorney for Middlesex County, Massachusetts, and I represent the law enforcement interests of approximately 1.5 million people who live in the urban, suburban and rural areas of the County. I am also proud to serve today as a representative of the National District Attorneys Association and am here to provide you with the views of that 7,000 member organization. In July of this year, our Board of Directors, representing all 50 States, unanimously passed a resolution supporting the need for such legislation.

Court authorized electronic surveillance is one of the most important and effective tools that State and local prosecutors have to fight and prevent crime. Often it is the only tool. In the past several years in Middlesex County, court ordered electronic surveillance has led to successful investigations and convictions of drug traffickers who poison our youth. In a series of wiretaps targeting extortion, loan sharking, and money laundering, we have been successful working with the FBI in penetrating the very highest levels of organized crime operating in Massachusetts and New England. Electronic surveillance was also used to prevent the escape from prison of a convicted murderer. These experiences are but a few examples of the vital importance of electronic surveillance to State and local prosecutors who conduct well over 50 percent of all court authorized wiretaps across this country.

I want to emphasize that electronic surveillance is a sophisticated, complicated operation no entered into lightly by law enforcement. In addition to the requirement

of a court order based in probable cause, most States require further administrative requirements to preclude abuse of the surveillance and there is frequently a requirement to make periodic reports to the court on the progress of the surveillance. There is also a significant financial and manpower requirement on the agency conducting the surveillance. Further, the telecommunications industry serves as part of the protective balance. I can assure you that local law enforcement does not have the capability to directly intercept telephonic communications and that the telecommunications industry will not provide the requested technical assistance in the absence of a court order.

I am here today to alert you to the fact that unless Congress intervenes legislatively, this vital and effective toll will be taken away from law enforcement and threaten public safety throughout this country. The problem is caused by advancing telephone technology which is making it increasingly difficult, it not impossible, to preserve the essential essence of electronic surveillance: the ability to identify, segregate and provide access to the specific calls of criminals who are the subject of court authorized electronic surveillance. Without that capability, court approved electronic surveillance will soon become a thing of the past to the benefit of criminals who victimize us, and who have access to and do not hesitate to use the latest technology.

While we as prosecutors welcome technological advancement and realize that the negative impact on law enforcement and public safety is unintentional, we believe a legislative solution is necessary. We urge you to act now. We support the administration's Digital Telephone Act of 1994, introduced by Congressman Edwards. This legislation simply requires telephone companies, when served with a court order, to continue to assist law enforcement as they have for the past 50 years by having the capability to identify, segregate and provide access to the conversations of specific criminals and target numbers, to the exclusion of all others, regardless of the technology, services or features involved. As prosecutors, we simply ask that our scientists and engineers put their unlimited talents to work in assuring that law enforcement is not left blindfolded. We support this legislative solution because it requires the telecommunications industry to meet the needs of law enforcement, but it allows the industry to decide the most efficient and effective approach.

The debate about the need for electronic surveillance has already taken place. The Congress and most State legislative bodies have resolved that, in certain cases, and only as a last resort, law enforcement may seek an impartial court order to perform limited electronic surveillance. We, as prosecutors, fully support this cautious, restrictive approach. Through this legislation we seek nothing more than to preserve the capability and you and the State legislators have already authorized and that is a vital tool in our fight against crime.

Mr. MARKEY. Thank you, Mr. Reilly.

And now we will turn to our final witness on the opening panel, Richard Metzger, who is the Deputy Chief of the Common Carrier Bureau of the Federal Communications Commission.

Mr. Metzger has become the expert at the Federal Communications Commission on the set of issues that we are discussing here today over the past year. We welcome you, sir. Whenever you are ready, please begin.

STATEMENT OF A. RICHARD METZGER

Mr. METZGER. Thank you very much, Mr. Chairman, Congressman Fields and other members of the panel. I appreciate this opportunity to appear before you today. I have submitted a written statement and I would just like to use my time here to summarize a few of the points I have made in that statement. I am here to discuss the role of the Federal Communications Commission as envisioned by the legislation.

Mr. MARKEY. Could I just ask you to move that microphone a little bit closer?

Mr. METZGER. I am here to discuss the role of the Federal Communications Commission as envisioned by the legislation in providing the assistance required by law enforcement agencies to main-

tain their ability to conduct authorized electronic surveillance in an era characterized by ongoing rapid changes in communications technology. The deployment of new facilities and technologies should not hinder the ability of law enforcement agencies to carry out their responsibility to protect the public and to detect and prevent crime.

Two of the duties that the legislation would assign to the Commission concern the establishment of technical standards and the resolution of disputes between law enforcement and a common carrier with respect to reimbursement for costs incurred by the carrier to comply with the legislation.

The role assigned to the Commission in these areas is consistent with responsibilities that the Commission has exercised in the past in analogous areas. In particular, the standards-setting process contemplated by the legislation is designed to rely principally on industry efforts to develop the technical standards necessary to provide these features and functions. Only if these efforts are unsuccessful is the FCC required to intervene.

The telecommunications industry in the past has shown that it has the ability to develop industry-wide technical standards that promote public interest goals. In the cellular area, for example, the industry worked to develop initial technical capability standards to ensure that customers could use their terminal equipment to obtain service in any cellular area. Those standards subsequently were incorporated into our rules.

The Commission's role in the resolution of reimbursement disputes similarly would permit the Agency to draw on its experience in regulating carriers' tariffed rates to fulfilling its responsibility under the legislation, again, not the area in which we would be applying a new standard under the legislation, but one which has required the Commission to become directly involved in complex economic questions in the past.

In short, while the legislation would require the Commission to address novel issues of considerable complexity, the issues relate to areas in which the Commission has historically exercised oversight responsibility. Because the duties assigned by the legislation are new, however, it would be helpful to the Commission in carrying out these new responsibilities that Congress could offer it as much guidance as possible in the exercise of those duties.

Finally, I want to stress, as Chairman Hundt has stressed in prior appearances before this subcommittee, and on this issue has conveyed to Judge Freeh, the Commission is prepared to offer any technical assistance that may be useful to the subcommittee in moving ahead with this legislation.

Thank you, Mr. Chairman

[The prepared statement of A. Richard Metzger follows:]

STATEMENT OF A. RICHARD METZGER, JR., DEPUTY CHIEF, COMMON CARRIER
BUREAU, FEDERAL COMMUNICATIONS COMMISSION

Mr. Chairman and Members of the Subcommittee: It is a privilege to appear before you today to discuss the role of the Federal Communications Commission in helping to ensure that law enforcement agencies continue to have the ability to conduct authorized electronic surveillance in today's era of rapidly changing telecommunications technology. In particular, I am pleased to have this opportunity to comment on the duties that would be assigned to the Commission under the legisla-

tion that was recently introduced, H.R. 4922 in the House and its identical counterpart in the Senate, S. 2375.

Court ordered electronic surveillance is a fundamental instrument in effective law enforcement. The rapid and expanding changes in telecommunications and the substantial changes that the industry continues to undergo provide sound premise to the legislation. The bills address the obligations of telecommunications common carriers and other members of the telecommunications industry to assist Federal and State law enforcement agencies in the interception of communications pursuant to court order. The legislation also commits discrete, yet important, technical and administrative responsibilities to the Commission in achieving the objectives of the bills. These new duties would require the Commission to resolve novel issues of considerable complexity, yet the role assigned to the Commission is consistent with its existing statutory obligation to promote the "safety of life and property through the use of wire and radio communication." 47 U.S.C. Sec. 151.

My comments today address the role of the Commission as envisioned by the legislation. There are a variety of issues relating to this legislative proposal that fall within the expertise of other agencies, such as the breadth of the legislation's coverage. As to these matters, it is important that Congress clearly resolve these issues in order to ensure that Congress, not the courts, establishes national policy in this sensitive area.

Judge Freeh has emphasized in his statements concerning the need for new legislation that court-ordered electronic surveillance is an integral part of the Nation's overall law enforcement effort. In the past, law enforcement officials, with the assistance of local telephone companies and other telecommunications common carriers, have been able to carry out authorized interceptions of communications without encountering significant technical difficulties. The fundamental changes in telecommunications technology in recent years have contributed directly to the explosive growth in both new telecommunications service offerings as well as information and other enhanced services that use telecommunications services.

The deployment of digital stored program control switches and installation of fiber optic transmission cable illustrate the pace of these technological changes. The percentage of digital switches operated by the Nation's largest telephone companies increased from 50 percent in 1989 to 80 percent in 1993. Both local and long distance common carriers also have implemented aggressive programs for replacing existing transmission facilities with fiber optic cables. In 1985, long distance companies operated approximately 20,000 miles of fiber optic facilities. In 1993, these companies reported that their fiber route miles had grown to slightly more than 99,000 miles.¹ Similarly, fiber optic transmission facilities operated by local telephone companies increased from more than 17,000 sheath miles in 1985 to over 225,000 miles in 1993.²

The growth in wireless services also has been remarkable. It was estimated at one time that by the year 2000 there would be 900,000 subscribers to cellular telephone service. Today, there are approximately 16 million cellular subscribers and the industry trade association estimates that by 1998 there will be 32 million cellular customers and 2.6 million customers of the new Personal Communications Service (PCS).³

These and other technological developments have enabled common carriers and other service providers to make available to American businesses and consumers an expanding array of telecommunications and telecommunications-based services. These changes, however, also form the basis for the request by law enforcement agencies for new legislation. As the wireline telephone network advances beyond analog switching and copper wire distribution facilities and efficient wireless communications systems are deployed in more than 700 metropolitan and rural service areas, law enforcement organizations have expressed serious concerns about their ability to conduct court-ordered interceptions of communications transmitted over these technologically advanced wireline and wireless networks. H.R. 4922 and S. 2375 seek to address these concerns through the concerted, cooperative efforts of government agencies, entities that provide communications services, and the manufacturers of equipment.

Briefly stated, the legislation would obligate telecommunications common carriers to meet certain "assistance capability requirements" by ensuring that their switching and other facilities offer certain features and services that are needed to assist law enforcement in conducting authorized electronic surveillance. The legislation

¹ Federal Communications Commission, Fiber Deployment Update. Table 1 (May 1994).

² *Id.* at Table 5.

³ Cellular Telecommunications Industry Association, "The Wireless Factbook", at 36 (Spring 1994).

would preclude law enforcement agencies from requiring specific system designs or the use of particular equipment. Instead, the bills would establish a process for developing specific, industry-wide standards. That process is designed to rely primarily on the telecommunications industry itself to prescribe the technical requirements that a carrier's facilities must satisfy.

The legislation establishes a 4-year period for common carriers to complete the necessary technical upgrades and other changes to their facilities. The bills, however, also empower the Commission to extend the implementation period for up to 2 years if it determines, after consultation with the Attorney General, that compliance with the specified assistance capability requirements is not "reasonably achievable." In addition, telecommunications common carriers would be eligible for reimbursement of "all reasonable costs directly associated with" the equipment changes and other modifications necessary to meet their obligations under the legislation for a period of 4 years after enactment. The legislation also provides for an assessment of penalties in the event that a carrier failed to comply with its provisions.

The legislation commits to the Commission four basic responsibilities: (1) to resolve disputes arising in connection with the industry's adoption of technical requirements and standards, or, in the absence of an industry consensus, to establish any needed technical requirements or standards and a time frame for compliance; (2) to grant, upon a prescribed showing, extensions of the time period to comply with the specified assistance capability requirements; (3) to determine, pursuant to the prescribed criteria, entities that would become subject to the assistance obligations because they have become a replacement for a substantial portion of local telephone service; and (4) to resolve disputes involving the costs for which a carrier is eligible for reimbursement by the government. The Commission will be able to draw on its experience in dealing with analogous issues in other substantive areas in carrying out the new responsibilities assigned by the legislation. To illustrate this point, a brief discussion of the Commission's role, as contemplated by the legislation, in the areas of standards and cost reimbursement is relevant.

The Commission historically has relied on the telecommunications industry to establish specific technical and design standards that achieve specified performance requirements and meet the service needs of telecommunications carriers and their customers. This approach avoids the problems that may develop if a government agency imposes specific mandatory design standards in an environment of ongoing, rapid technological change, such as foreclosing unnecessarily industry-based research and development activities that could provide new solutions to technological challenges. Moreover, voluntary standards-setting bodies, which are often utilized in the telecommunications industry, have shown that they can develop efficient, innovative solutions to identified needs. To promote a robust cellular industry, for example, the industry in 1981 developed the initial cellular compatibility standards, including radio-system parameters and call-processing procedures, to ensure that cellular customers can obtain service from any system.

The legislation generally follows this approach. The bills set out particular performance standards that telecommunications carriers would be required to achieve, but the industry is given latitude to develop the precise technological solutions that will meet their "assistance capability requirements." Moreover, law enforcement agencies are expressly barred from requiring or prohibiting specific design features, services or systems configurations. All parties, including telecommunications standards-setting organizations, industry associations and law enforcement agencies are directed to consult to promote efficient industry-wide implementation. The Commission is required to intervene in the standards-setting process only if these efforts are unsuccessful.

Disputes involving the technical standards applicable to "assistance capability requirements" would be substantially more complex than those the Commission has had to address in the past. The Commission, however, would not be starting from a blank slate. Rather, the record developed in the course of the industry's efforts to establish the necessary standards would provide a starting point for the Commission's consideration of the unresolved issues. Simply put, if the consultative process outlined in the legislation failed to resolve all of the standards issues, the Commission can devote the resources and expertise required to carry out its responsibilities.

The legislation also would assign to the Commission the responsibility for resolving disputes concerning the reimbursement of carriers for costs incurred in providing "assistance capability requirements." To a large degree, this assignment would invoke the Commission's traditional role of ensuring the rates charged by carriers to their ratepayers are "just and reasonable." The FCC has gained substantial experience over the past decades in evaluating cost information submitted by local and long distance carriers to justify the rates they proposed. Although the legislation would require the Commission to apply a different standard to resolve disputes be-

tween carriers and the Attorney General, the experience and expertise of the Commission's professional staff in addressing complex economic and technical issues raised by carrier rate filings will enable the Commission to fulfill its obligations under the legislation.

It also is worth noting that the Commission's review of carrier proposed rates is conducted in a public proceeding in which all parties have ample opportunity to present their views. The Commission's determinations are rendered on the basis of the public record developed in the proceeding. Thus, the Commission will have the benefit of the analysis and recommendations of all interested parties in reaching its decisions.

The cost of compliance connected with this legislation, and how it should be allocated, are fundamental questions whose resolution impacts the extent of the Commission's responsibilities. It is difficult to provide a clear perspective in this area. This emanates from the inability to determine the capacity needs of law enforcement and the consequential performance requirements of the telecommunications carriers. The legislation takes the first step toward resolving these issues by requiring the government to estimate its capacity needs and industry to commence establishing technical standards. In fulfilling its responsibility, the Commission would benefit from further guidance in this area.

Moreover, structuring a mechanism that reflects a fair environment where all competitors retain opportunities, yet receive no advantages, is what is sought. The legislation provides a 4-year window, with the ability to obtain a 2-year extension, to make the modifications necessary to comply with the capability assistance requirements and to seek reimbursement. In terms of both compliance and reimbursement, one of the elements to consider is the changing environment of the telecommunications industry. The industry is moving beyond the historical monopoly ratepayer concept. Moreover, although we anticipate that technological and regulatory changes with coming years will create opportunities for new entrants, the present reimbursement plan essentially applies only to existing telecommunications carriers. Maintaining a proper competitive balance in these evolving markets may entail a commitment of discretion to the Commission to consider particular circumstances. To the degree that the Commission is to play a role in seeking to bring about a balance, it is important that the law clearly set forth the factors that should be weighed.

In sum, the legislation sets forth specific responsibilities for telecommunications carriers to provide assistance to Federal and State law enforcement agencies. It also establishes a time period for the carriers to implement the equipment and other modifications required to meet its assistance responsibilities and provides a mechanism for reimbursing carriers for the costs incurred in making those modifications during the 4 years after enactment of the legislation. The role assigned to the Commission by the legislation is consistent with responsibilities that the Commission has exercised in the past. We will continue to be available to provide the subcommittee any assistance as this legislation moves forward.

Mr. MARKEY. The gentleman's time is expired, and now we will turn to questions from the subcommittee members of our first panel, and the Chair will recognize himself for a round of questions.

Let me begin by asking you, Mr. Freeh, the debate as we will hear from the second panel revolves, to a very large extent, around the cost of the installation of the new software and hardware that will be necessary for law enforcement officials to continue to conduct their business as they have in the past, that is, to upgrade from analog to digital as we move into this new modern telecommunications era.

The legislation calls for \$500 million to be expended for these purposes. The FBI and other law enforcement agencies contend that will be more than adequate in order to deal with the technological upgrade which is needed.

On the other hand, the communications companies argue that it is a vast underestimate of what the ultimate costs will be.

Could you give us your justification for maintaining the \$500 million will be adequate and then we, on the second panel, can

pose the same questions to the telecommunications executives so that we can have this issue out and the members of the committee can then deliberate over the appropriate number that we should rely upon.

Mr. FREEH. Mr. Chairman, as you point out, it is a singularly important issue. When we suggested initially, as we maintain now, a projected cost of \$300 to \$500 million, we, unfortunately, do not have a crystal ball and there are no specifics with respect to the out-years as to what this will cost.

By the same token, the industry has more or less, from our point of view, speculated in the other direction, perhaps, when they talk about billions and billions of dollars. I think the prudent course is the finding of the GAO report which suggests that the ultimate cost of this fix will depend precisely on the solutions that are ultimately imposed, the efficiency with which the industry and the government collaborate on their resources, on their research abilities, and of course the objectives and the time frames within which this is to be accomplished.

In a way, the law enforcement agencies represented here and around the country are really soldiers who are waiting in this case for somebody to pass them the ammunition. We don't have, on one level, a great stake in debating whether the ammunition comes from the government for the first \$500 million or from some other source, the private sector, for instance, for additional ammunition.

I think the incredibly important issue here is that everyone has made the finding that there is a problem that has to be fixed. Everyone with sincerity and good faith wants to fix that problem. Our view is that the \$500 million will be substantial to fix it.

I noticed yesterday that AT&T Bell Labs was awarded their 25-thousandth patent which keeps them with their patent a day motto. I am sure within the incredibly talented pool of people we have, not just in the industry, but whether somebody is studying at MIT or Osaka, there is going to be a solution, because it is a software solution, to this very intractable problem, and I was disturbed on Friday when one of the industry representatives referred to the \$500 million as chunk change. I don't see it as chunk change.

We see it as a very extraordinary effort by the government to fund a public safety issue. Nobody would think, for instance, today of having a manufacturer design for consumer use an unsafe product. We don't even need legislation to make that projection.

I think that after 4 years or with the extended 2 years, if there is a need to go beyond the \$500 million, as the bill proposes, that is a cost which should be borne by the industry. They should not be providing and using services and features that are unsafe. If they have services and features that don't allow the police and law enforcement to protect people, those are inherently dangerous products, and I think at that point, the industry has an obligation to work for public safety in the same regard.

Mr. MARKEY. I guess my view of this is somewhat educated by the experience which this subcommittee had with the Americans with Disabilities Act back in 1990 when, for the deaf and hard of hearing community, this subcommittee mandated that every television set have built into it a chip which would allow for closed cap-

tioning to go across every television set sold in the United States after 1993. Our expert witnesses from the industry told us it would cost \$25 a television set. Well, it wound up costing \$3 a television set, dramatically lower than we were told it was going to cost, and moreover, it has built in huge capacity on that computer chip to do many other things as well with television sets across the country.

So I think it is important for the subcommittee to make some determinations as to what is an adequate projection for cost here, especially with the advances which are being made in software and hardware on an ongoing basis.

So, again, back to the question though of who should bear the cost, the taxpayer or the ratepayer; if I heard you correctly, you are letting that decision be made by the subcommittee, by the Congress, rather than a view expressed by the FBI; is that correct?

Mr. FREEH. Yes, I think that is correct. I mean to the extent you want to distinguish a taxpayer from a ratepayer, and I think that is a legitimate distinction, I do think that is a decision left to Congress, but I do think there should be some clear finality at some point because I think that is the motivation for industry to be as effective as they can be, and to force us to ensure that only our most basic and critical requirements are dealt with and not features we don't need.

Mr. MARKEY. And Mr. Reilly, I would like to clarify one of the points which you made. You said that in fact this does not in any way increase the wiretap capability of law enforcement officials, but rather deals with the advances in technologies so that law enforcement officials do not see an erosion of their existing capability legally to wiretap.

Could you expand upon that for us, please?

Mr. REILLY. Absolutely, Mr. Chairman, absolutely. We are trying to maintain the status quo. In this entire country, there are less than 1,000 wiretaps that are conducted in the course of a year. There is a reason for that.

We have to go through a very rigorous process to obtain a wiretap. It has a requirement of probable cause, the requirement of an affidavit. It is submitted to a judge, approved by a judge, with restrictions that are placed on that. There are periodic reporting requirements in which we have to go back to the court and to report to the court and to continue to justify this intrusion.

In addition to that, it is a very expensive proposition in terms of manpower and the financial resources of an office. So it is not something to be taken lightly. So this will not increase one iota the number of wiretaps in this country.

It will just allow us to continue what we have been doing, sparingly, yes, but effectively for the past 50 years, and to allow us to continue to do that. If this continues the way it is going right now, we are being constantly frustrated, slowed down, and sooner or later, although we have not faced it personally and maybe the other agencies have, there has not been a life and death situation, but there will be a time where we will seek a court order and we will obtain a court order, a court-authorized wiretap to allow us to overhear the conversations of a particular person, and we will not be able to implement that because of the developing technology, and the other problems that the industry is having in enforcing

that court order, and that will be obviously a problem, a public safety problem that I don't think this Nation wants or this Congress wants. That is the data that we are facing in the future.

Mr. MARKEY. Let me follow up on one other point that you made. You said that there are 1,000 wiretaps per year in the United States, more or less.

Mr. REILLY. Yes. Probably 800, 900.

Mr. MARKEY. How does that break down geographically in the United States?

Mr. REILLY. I can—perhaps the Director can speak to the national statistics. I can state that in our jurisdiction, which is the largest county in Massachusetts, and we are fairly active, we are limited because of the restrictions and the rigorous process that we have to go through and the sheer expense of this to probably an average of 3, 4, 5 a year. So it is not something that is done—that is done often.

Mr. MARKEY. Perhaps Mr. Freeh has the information which can help us to understand the profile of these wiretaps across the country.

Mr. FREEH. Surely. I don't have a regional breakdown; I can provide that to the committee later today.

On a State, local versus Federal basis in fiscal 1992, there were a total of 919 wiretaps. That is all Federal, State, and local across the country. The Federal Government was responsible for 340 of them, State and local authorities, for 579. Of the 340, the FBI performed 74 percent.

In 1993, the total number was 976. The Federal Government is responsible for 450, the State and local is responsible for 526. Actually, between 1992 and 1993, the FBI has done less wiretapping, going from 74 to 71 percent of the Federal wiretaps. The State and local authorities have increased from 27 to 33 percent between 1992 and 1993.

Mr. MARKEY. And again, if you could help us understanding geographically how they break down across the country. Is there a concentration with regard to the organized crime or the types of activity that the district attorneys and the FBI might be tracking disproportionately compared to other types of crimes?

Mr. FREEH. Yes, absolutely. In the northeast, particularly the New York City metropolitan area, also in the New England area, Boston in particular, in the southeast United States, Florida, Texas, the California districts are clearly the heaviest ones, the northern district of Illinois for concentrations of wiretapping orders.

Mr. MARKEY. Thank you.

Mr. REILLY. In terms of a case, to follow up on it, our typical case would be to target a major drug trafficker or organized crime, so those are the areas that our main focus would be on a local level.

Mr. MARKEY. Thank you. Thank you. My time has expired.

Let me now recognize the ranking minority member, Mr. Fields.

Mr. FIELDS. Thank you, Mr. Chairman.

Director Freeh, first of all, I want to just begin by congratulating you on that outstanding job that I think you are doing, and I said privately yesterday, and I will say it publicly, I thought what you did at Russia was just outstanding, and I also want to congratulate

you on communicating to members of this subcommittee not only personally, but I know I discussed this with your field agent in Houston, with local DEA, Customs, local law enforcement, and I think that is valuable for members to have that kind of contact to understand the problem, and what I would like for you to do if you could, and this may not be a question you can answer, and if you can't, I will certainly understand, but to give us an understanding, in your testimony you talk about 183 frustrations.

Could you give us some kind of understanding of what you are talking about when you say you were frustrated in a wiretap effort?

Mr. FREEH. Yes, I will be happy to, Congressman Fields. The breakdown that we have provided goes into certain general and a few miscellaneous categories. Our survey, which was a survey done informally, although with many Federal, State, and local law enforcement agencies, showed that in 54 cases, the cellular port capacity frustrated the execution or the obtaining—I am sorry, the execution of wiretap or court orders.

In 33 cases, there was an inability to capture dial to digits contemporaneous with audio recordings. Four cases, the cellular provider could not intercept long distance calls or provide call setup information to or from a targeted phone.

In 20 cases, the order was frustrated by speed dialing, voice dialing, or call waiting, 10 cases frustrated by call forwarding, four cases frustrated by the direct inward dial trunk group, and I would have to explain that to you in some other form because I don't quite understand it myself.

Voice mail I do understand, 12 cases where we were frustrated in operating the order. With respect to 42 other miscellaneous orders which were frustrated, they range from inability of the provider to provide tap and trace information, inability of the provider to isolate digital transmissions, other calling features, such as callback, inability of the provider to comprehensively intercept communications and provide setup information.

These do not, of course, include many instances, and we have several of them, which I can provide in a letter to the committee, where prosecutors and agents did not seek court orders in particular districts because of the inability of the carrier and telephone companies to provide the particular targeted service.

Mr. FIELDS. Is it your analysis that this legislation would respond to these frustrations?

Mr. FREEH. Yes, absolutely over time would respond to them and correct them.

Mr. FIELDS. As well as, I understand in my discussions, you have a telecommunication industry that wants to cooperate and it appears that the central issue, correct me if I am wrong, but the central issue really goes along the line of what the chairman was asking in his line of questioning, and that is cost, and it seems that there is a disparity between the amount in the legislation, the \$500 million, and what the GAO suggests the cost could be, and it also appears that from what you said just a moment ago, much of the wiretapping that is done is located in particular, identifiable regions of the country. So my question is: Is there a possibility of

prioritizing, either in time or scope, how the intent of this legislation is carried forward?

Mr. FREEH. That certainly is a discussion that we have had with the industry, and just to follow up on a point that you just made, I compliment the industry for working as hard and as diligently as they have to solve this problem.

We are not adversaries on this issue. For 25 years in implementing Congress' decision to authorize wiretapping, the carriers and the providers have been our natural allies and we have an excellent record of cooperation.

We have discussed the possibility of grandfathering or phasing in continued access in areas where we have a greater proportion of need. The danger with that is that it does perpetuate vulnerability. Just to take a for instance, a kidnapping that occurs in a place that may not be the subject of intense organized crime or drug trafficking activity may be an area where we feel temporarily confident to forestall or postpone this technological fix. Suddenly we have a kidnapping, we have someone who is threatening to put cesium into a water supply. We have a transnational group of criminals deciding to operate. We have a terrorist activity. I think by grandfathering and phasing in compliance just perpetuates a window of vulnerability which gets greater and greater as time goes on.

So my recommendation to the committee and to Congress, which is consistent with the bill as introduced, is to not tend towards a grandfathering solution, but to have a complete and at some point final period within which everyone is protected, because the lives at stake here, I think, are really substantial.

Mr. FIELDS. One aspect of my prioritization question is just the realization that technology is changing so quickly, and there is going to be so much additional deployment in the next several years that I was wondering if that, in fact, had been taken into consideration when you were discussing it.

Mr. FREEH. Yes, it has. In fact, with respect to the capacity problem, the legislation, as you know, provides that that is one continuing cost, the cost of capacity, which the government will absorb because of the changing technology and the possibility that capacity may be necessary to be increased in a particular area.

Mr. FIELDS. Is there anyone within the law enforcement community who disagrees with this legislation?

Mr. FREEH. No. I mean, I have been in this business a long time. There are few and rare unanimous issues in terms of importance and critical need, and this is certainly one of them because lives are at stake.

Mr. FIELDS. I want to say to the people who came to my office in Houston that in the time of my service, I have never had a group come in in a unified fashion. I think you referred to this as a drop-dead piece of legislation, that you have to have it, and I have never had law enforcement come in and say something is a must, and that was impressive to me, and I assume that is your feeling and the feeling of the community at large.

Mr. FREEH. Yes, sir.

Mr. FIELDS. Thank you, Mr. Chairman.

Mr. MARKEY. Gentleman's time has expired.

The Chair will recognize the gentleman from California briefly for a unanimous consent request.

Mr. LEHMAN. Thank you very much, Mr. Chairman, and I have a statement I would like to insert in the record and express my interest in this issue. I hope we can go forward and satisfy the problems that the Bureau and law enforcement have for the need to do their job and at the same time not disrupt our ability to go forward here on the information highway. I think everyone has the same goals; we can solve this problem.

I thank you.

Mr. MARKEY. And with unanimous consent, we will include the gentleman's statement in the record at the appropriate point. Gentleman's time is expired.

We now recognize once again the gentleman from Virginia, Mr. Boucher.

Mr. BOUCHER. Thank you very much, Mr. Chairman.

Mr. Freeh, let me pursue with you just for a few minutes several other aspects of the question of cost and who will bear cost in certain circumstances. I very much appreciated your suggestion in response to Chairman Markey's question that as between the general taxpayer on the one hand and the ratepayer on the other hand, that this is a decision perhaps that we should make in the Congress and that you would accede to whatever decision we made in that regard, and I do appreciate your statement to that effect.

Will that also, do you think, be the view of the administration? Do you speak for the administration in that regard, and if not, who should we talk to?

Mr. FREEH. Well, I can say certainly for the administration that there is a firm commitment to pay and reimburse for this effort \$500 million, which is an extraordinary amount given the speculation that currently exists as to how much it may cost to fix.

Again, the cost-bearing issues have been, as you know, and as you have provided very good counsel to us, an issue which is probably the only issue needing to be resolved. The other debates as to the need for wiretapping are not seriously contested.

I am very hopeful that in the next 2 weeks, this issue can be resolved, but I think ultimately it is a decision for Congress and I think—you know, it depends on how you put the question.

If you ask Americans whether they want a FBI wire tax in their phone bills, they will say no. If I asked them whether they want a feature on their telephone which allows me to find their child if they are taken, they will say yes. I think it is a question of perception.

Mr. BOUCHER. Well, I take it that for present purposes, you do speak for the administration in certainly presenting views before this committee and we can assume, therefore, that the administration's view, until we learn to the contrary, is that if we make a decision that this cost should be borne by the taxpayer as opposed to the ratepayer, that the administration will agree.

Let me ask you about a couple of aspects again of the cost question relating first to the short-term and then to long-term costs. It is unclear when one reads the bill today upon whom the cost would fall in the event that either Congress does not appropriate the \$500 million necessary during the 4-year transition period in order to

perform the required equipment modifications, or if the ultimate costs of performing those modifications turn out to be more than the \$500 million, or in fact whatever amount Congress in fact appropriates.

Then the question is squarely presented to us, who will bear those costs. Will it be the industry or will it be the government? Now, is it your understanding that what the bill should be saying in this respect is that within that 4-year period, those costs should be borne by the government?

Mr. FREEH. Up to and including the \$500 million figure?

Mr. BOUCHER. The \$500 million.

Mr. FREEH. Yes.

Mr. BOUCHER. But assuming appropriations in that amount are not made, then the burden would not shift to the industry, in your view, would it, that they should perform equipment modifications without reimbursement?

Mr. FREEH. Well, if you look at the statute, I think it is drafted currently to read that in that contingency, a judge on the application of the government, for instance, would have the discretion to decide whether the lack of reimbursement falls within the reasonable circumstances which would exempt a carrier from mandated compliance. I think that is the current proposal in the legislation.

Mr. BOUCHER. That is correct, and I guess I am questioning the wisdom of that and asking you for your counsel on the wisdom of that as well, because the potential very clearly is created that even within this 4-year transition period where we know there are going to be costs, that the industry might have to bear those costs in the event that appropriations are not made or that the ultimate costs exceed whatever appropriations are made.

Is that wise, do you think? Should we be imposing that charge on the industry?

Mr. FREEH. I am not as concerned about it as perhaps—as you are, sir, and other members might be. I cannot conceive of the Executive Branch not assuring, of course, with the ultimate decision being with the Congress, of providing the necessary funds to provide a public safety protection which everyone is in agreement has to be ensured.

I would be shocked if we moved forward and we had the authorization that the funds, at least for the first \$500 million, were not forthcoming.

Mr. BOUCHER. Well, knowing the difficulty that we have for obtaining funds for virtually any discretionary programs today, given the kind of budget caps that are in place, I would not be shocked if that precise circumstance arises, and I think the difficulty is, if it does arise, we are only inviting protracted litigation to the disadvantage of all parties concerned, and it seems to me that at least for this transition period, we ought to write these rules very clearly and specify precisely where these costs will fall in the event that Congress does not provide the requisite appropriations. We will have a further discussion about that later.

Let me inquire with respect to another area, and that is the long-term costs. The bill clearly places those long-term costs on the industry, on the presumed theory that the new equipment can very

conveniently have these modifications designed and manufactured into it, and therefore the long-term costs will be de minimis.

Do you have any evidence that supports that theory or makes any estimates as to what these costs in fact would be?

Mr. FREEH. I don't have any scientific or specific results which I could share with you today.

Mr. BOUCHER. Let me ask you this then, Director Freeh. Is it possible that those long-term costs could, in fact, be fairly substantial?

Mr. FREEH. The possibility exists that they could be.

Mr. BOUCHER. OK. That is the simple answer I was looking for. I think, again, we have to have discussions with regard to how we handle those costs just as we do for the short-term ones.

One final question and then my time will have expired, and that relates to coverage. I mentioned this in my opening statement, and would simply ask if you have any comments with regard to the situation of the shared tenant facilities, where the owner of an office building provides telephone connections within that office building for the various tenants who take part in it, and then of course that goes well with a single building, it is easy to assume that that kind of practice and network could be expanded to other buildings until before very long you have got a fairly sizable network operating in competition with the local exchange carrier.

As I read the legislation, that private network is not a common carrier, it is not a mobile offerer of telecommunications service, therefore, as I read it, it is not covered by the equipment modification provisions, creating the potential for anti-competitive advantages with respect to the covered network, creating the possibility that you as a law enforcement agency could not perform the wiretaps you would have to in that private network.

Now, should we leave that circumstance as it is or does that call out for being addressed?

Mr. FREEH. I think for now we should leave it where it is. First of all, from the beginnings of this proposal, not only within the administration, but with all of the industry representatives, and certainly for the last intensive 6-month's worth of negotiations and representations, it has been clear that the private networks, the private communication networks, the PBX operators, have been explicitly excluded from this coverage.

Yes, in a perfect world, not only should those networks, but probably a lot of other potentially growing areas, should be included. My view right now is that given the representations that have been made in the discussions, to do that at this late juncture would scuttle a very critical proposal.

Also, with respect to our immediate needs and even our long-term needs, the universe of dangerous criminals who are specifically targeted by this specific technique are well within the common carriers network. Sure, it is incomplete by exempting certain private networks, but it is a very, very small and insignificant minority at this point and in the projected future.

Mr. BOUCHER. Thank you, Mr. Freeh.

Mr. MARKEY. The gentleman's time has expired.

Let me suggest a way to proceed at this point. There is a roll call on the Floor. There are about 11 minutes left to go on the roll call.

What I would like to do is to recognize right now the gentleman from Ohio, Mr. Oxley. Mr. Wyden has already left to make this roll call. He will come back and continue to chair the committee so we will not take a break, and then I will go over with Mr. McMillan, return, and recognize Mr. McMillan on his own time.

So at this time, I recognize the gentleman from Ohio, Mr. Oxley.

Mr. OXLEY. Thank you, Mr. Chairman, and I appreciate the expeditious way that this is going to be handled.

Let me first of all ask both Director Freeh and Mr. Reilly, just so that we are clear on this and the public understands, do either of you seek to expand in any way current law with respect to wiretap authority under this bill?

Mr. FREEH. No, that is not contemplated in the bill and certainly would not be even a logical or practical consequence of this technological correction.

Mr. OXLEY. Mr. Reilly.

Mr. REILLY. That is not our intent at all.

Mr. OXLEY. Let me ask you both this question. Do you feel comfortable under the current regime of seeking and acquiring wiretap authority as set out by the statutes and the courts?

Mr. FREEH. Yes, I do. As Mr. Reilly pointed out, it is an extremely rigorous and difficult technique to have authorized by a court, but we subscribe to those strictures precisely because of the sensitivity of the technique, and from the Federal Government's point of view, and I am sure Mr. Reilly's point of view, we are quite comfortable and supportive of the current regime.

Mr. OXLEY. I am not sure I know the answer to this. What is the liability or the potential liability of a law enforcement agency should they be deemed to be violative of the current statutes and the court decisions?

Mr. FREEH. From a procedural and evidentiary point of view, the fruits of such a surveillance conducted without compliance to the order or the other statutory protections would be evidence suppressed in a criminal proceeding.

On a personal liability basis, if acting outside of the scope of their employment, there could be civil liability, there could clearly be criminal liability even for Federal law enforcement officers who abuse electronic surveillance inconsistent with the statute. There is a specific criminal provision.

Mr. REILLY. In our State, there is both criminal and civil liability, and obviously you would be jeopardizing the case itself, and I think that I speak for all the prosecutors in this country that we agree that there should be a rigorous approach to this and it should be regulated by the courts and only authorized by the courts. We agree with that and will abide by that.

Mr. OXLEY. So the exclusionary rule would indeed apply under those circumstances and be subject by a motion to defense counsel under those circumstances?

Mr. FREEH. Yes.

Mr. OXLEY. I am also interested in following up a bit on Mr. Boucher's questioning, that is, instead of focusing in on what the provider is or who the provider is, whether we should try to focus in on who provides the service.

That is, with our telecommunications legislation that we have already passed in the House and hopefully we will get to the President this year, we are essentially opening up this so-called local loop and that there will be a lot of providers, we envision, in a competitive mode. So you are going to have long distance companies, you are going to have alternate providers, you are going to have cable, and it seems to me that if we are to stay ahead of the curve, we ought to be focusing our attention on the service provided as opposed to the telephone company over here and ignoring some of the very real competitive forces that are going to be into that marketplace.

Do you have any comments in that regard, Director?

Mr. FREEH. Yes, I think that is exactly right. I think if you take the instance of the World Trade Tower building which does offer a private telecommunications network for its customers, if we are talking thousands of such customers and services offered to the public, we would view that, and I think the courts would view that service, as being consistent with the definition of a common carrier. So I think even within some of the private networks, as they grow and mature and particularly when they offer services to the public, we will be covered more and more as those services become identical to the services offered to other consumers.

Mr. OXLEY. I am informed that at least for the last 5 years, the security officials with the major telephone companies have been aware of the problem, not just the potential problem, but the real problem of wiretaps and securing that.

Why was this problem, in your estimation, allowed to persist for that long a period of time? Don't the providers feel a certain responsibility under these court-ordered wiretaps? And what efforts have been made from the private sector, that is, the carriers, to help solve that problem?

I know that you gave them some praise for being cooperative in this effort, and clearly over the years they have been, but shouldn't somebody have seen from their perspective, seen the technology changing rapidly and moved to address that?

Mr. FREEH. Well, before I became FBI Director, representatives of the FBI, as well as State and local enforcement authorities, have been alerting the common carriers to this problem for at least over the last 4 years, so this is not news for them.

I am very hopeful, and I think one of the reasons that I think the \$500 million cost is reasonable and that extraordinary costs beyond that, although possible, are very highly unlikely is because I have to believe that as responsible corporate citizens, they have been cognizant of this problem certainly over the last 4 years and have taken some preliminary steps to engineer and upload the necessary features to correct this problem.

I would be surprised, and I don't think this is the case, that they have done nothing in that regard. In fact, some of them we know have taken specifically some steps to correct this problem.

Mr. OXLEY. Lastly, in your discussions with Congressman Fields regarding the potential at least of phasing in your ability, and obviously that is driven by cost. That is, from a policy standpoint, what would be wrong with phasing in the capability, wiretap capability, in the areas that are most sensitive to your needs?

I mean, it is obvious, I think, that wiretap authority would be much more likely and needed in Boston or Chicago or New York as opposed to Findlay, Ohio. And if that is a cost factor, doesn't it make sense that we would deal with the areas of need first before we deal with the rest of the system?

Mr. FREEH. Yes. If limited by cost, it certainly would make sense and would be prudent to proceed in that way. One of the problems, however, is that as the telecommunications systems become more sophisticated, telephony and personal communications systems, the bill itself contemplates the handing off between cellular companies, for instance, of communications from one local carrier to another.

If we have a large vulnerability between two areas where we have heavily invested our earlier funds, we could still be at risk in terms of covering the network which will move not just between the main areas where we have concentrations of originating wiretaps, but where calls will soon and currently transit.

Mr. OXLEY. Thank you. Thank you, Mr. Chairman.

Mr. WYDEN [presiding]. I thank my colleague, and Director Freeh, I think at this point you have heard that essentially all the members are supportive of this effort to ensure that law enforcement has the tools to do what it needs as it goes into the next century to protect our citizens.

I think that what the debate is about and how I would state it is essentially about accountability. The view here is that if you go through the congressional appropriations process, you have an open debate, you can have a discussion about priorities and I would, for one, be supportive of the kind of thing you are talking about.

If you don't go through the congressional appropriations process, you have got a situation with the ratepayers where, in effect, everything can sort of be buried and you get into what I described earlier as the kind of hidden tax situation.

So let me ask you about the first part of the bill that concerns me. You have got the view that you are going to, in the initial period, get the appropriation and that is essentially going to handle the bulk of the matter, and your view then is that the additional kinds of services, the additional enhanced capability, would be, in your view I guess, de minimis; it would be a small expenditure.

My question is: what happens if it isn't and how do we proceed in terms of this legislation to try to deal with that prospect so that we can stand up at town hall meetings in Portland and North Carolina and everywhere else and describe a process that people will say is straightforward and accountable?

Mr. FREEH. I agree with you that the appropriations process is ideally suited for that accountability, but even if the \$500 million were to be immediately appropriated, Congress, I am sure, and we certainly would encourage them, would follow the expenditures very carefully.

The \$500 million will not be expended within a 12-month period or within a fiscal year period. That will be the subject of continuing evaluation, not just by the companies who are seeking reimbursement, but by the Congress which has authorized that money. So I think that is a dynamic process which will occur.

Mr. WYDEN. I guess my question is, what about after the \$500 million? That is what I am particularly concerned about. I agree

with the point that you are making. I am concerned about that down the road kind of situation and how we can show that the Congress is acting in an accountable fashion to the public after that \$500 million.

Mr. FREEH. I think it is quite responsible, with this particular scenario contemplated, that after an expenditure of half a billion dollars over 4 years, that the industry does become somewhat responsible in insuring that the mandate is continued.

I think the difficulty with leaving vague or with guaranteeing the government payment in perpetuity is really a motivation not to be as efficient as everyone can when they know that the reimbursement is going to run out in 5 years.

It is the same issue, I think, with respect to mandating corporations to be responsible with respect to protecting the environment. No one could contemplate either now or 5 years ago or 10 years ago from when the Clean Air Act was passed what the cost would be in following the mandate that Congress set down for providing clean air and clean water.

At some point, the corporate citizen has to become responsible for that maintenance, and I don't think it is irresponsible for Congress to say that after half a billion dollars, the industry is then responsible for continuing a mandate which ensures public safety.

Mr. WYDEN. I think what I am driving at is that the efficiency you are talking about makes a lot of sense, but the best way to ensure efficiency is to, in effect, say you are limited in terms of what you can buy to what you have the money for, and I am concerned that we are starting down a path where people can buy without getting the money.

Now, we are not going to hash through all the details today, and I appreciate how open you have been in terms of dealing with this, and I think you have heard a number of members pummel this question at this point, but understand that that is what the debate is really about.

The debate is about accountability and in effect not signing a blank check in perpetuity which would encourage, at least in my view, some of the inefficiencies and perhaps some extras that wouldn't be essential to the valid law enforcement concerns that you are trying to carry out.

My question, I guess, at this point would be for the FCC as well, and this deals with the technological capability. Is it the view of the FCC that the phone companies would have the ability to build these costs into the rate base if there was not some other way that Congress specifically stipulated to go about financing these capabilities?

Mr. METZGER. Well, Congressman, I think to emphasize the point you just made, what the Commission would look for is guidance from Congress as to how this issue ought to be resolved. This is an important issue that is really the Congress' to make rather than the Commission's.

With respect to how the industry might go about it, I assume, as I read the legislation, what it contemplates is as we go forward in the future and new technology is deployed, new switches are developed and so on, the incremental cost of adding a particular feature or function would be quite small, and therefore to the extent

it is reflected in the overall cost of a facility, the actual incremental cost of that feature, having been planned for from the beginning, would be relatively small.

Mr. WYDEN. In absence of any Federal definition here and a clear kind of standard, isn't there a good chance though that the States and the State regulators might in effect let these costs be passed on to the consumer?

Mr. METZGER. Well, certainly to the extent that the State exercises regulatory jurisdiction, they would have to review the costs underlying their rates and that would be for the State commission to determine; that is correct.

Mr. WYDEN. My understanding is that it would be a legitimate cost of doing business and the States would pass that on. Is that correct?

Mr. METZGER. That would certainly be their determination to make, yes.

Mr. WYDEN. Let me ask you one other question. Maybe Director Freeh, we can get into this. I was sitting, as I heard our colleague, Jack Fields, make what I think is an excellent point about the geographical spread of these wiretaps in thinking about how folks possibly in John Day, Oregon are going to end up paying for it, and my understanding is that at this point, statistics are something like 50 percent of the wiretaps are in two States, 80 percent in six States, and—at least that is the number for the cellular wiretaps, 50 percent in two States and 80 percent in six States.

Isn't this a pretty compelling argument, as we try to wrestle with the cost issue, for pursuing some version of what Mr. Fields has asked about, to have some manner of priority setting or targeting as we begin this effort?

Mr. FREEH. I don't know that I have the technical expertise to answer this question. My understanding of the technology is that it is a baseline capability.

If it is a baseline capability technology that needs to be developed, that is the substantial and overwhelming cost. Once the technology is developed, the deployment of that technology to a wide array of venues, including those outside the districts where we do most wiretapping, I think is really the insubstantial part of that cost.

I think it is the technology, more than the physical location of its manifestations that is the main cost, and again, with the increasing crime trends and the somewhat murky picture about predicting where in 10 years, for instance, we are going to have the greatest concentrations of crimes, you know, 5 years ago, places in the Midwest cities that were strangers to crime now have gang populations and skyrocketing crime rates, so I think it is pretty hard to project with any kind of comfort where we could best not be.

Mr. WYDEN. I think that is a valid point, but as we saw in the crime bill, there is tremendous concern on the part of small cities and local governments about these uncharted kinds of Federal initiatives, and I am anxious to work with you on this.

It is clear that the Bureau is being open in terms of trying to look at various financing arrangements, but this is a national mandate that the Bureau is talking about, and yet the numbers indi-

cate a disproportionate amount of the need is in a small number of areas, and we are going to have to think of some ways to keep small towns and other communities from getting buried in this and I am anxious to work with you on it. My time is expired.

The gentleman from North Carolina has been waiting.

Mr. McMILLAN. Thank you, Mr. Chairman. Just on the geography, is it true that wiretaps may tend to be geographically concentrated. They are concentrated because you may be focusing upon a wholesale or retail source, whereas the ultimate distribution of the drug, hence the adverse benefits or effects that we are trying to deal with, may be widely distributed all over the country in places where there are no wiretaps available. So I think maybe that is trying to draw too fine a distinction here.

Another distinction which I think we are wrestling around with is the difference between the consumer and the taxpayer. If any person who has a telephone doesn't think they are a taxpayer, just look at their statement. You can start with that. The excise tax is quite substantial, and I know there is a reluctance not to increase it.

The fact is we are operating under caps on discretionary spending. The administration has projected a budget for 5 years in which discretionary spending froze. So if we are going to find 500 million bucks, it is going to have to come out of somebody else's hide somewhere, probably the consumers, because we are the taxpayer.

Now, there may be some incidences here and there, but I don't think we should worry too much about that. I think we do need to worry though about getting this thing funded at the outset, and I don't think there is any argument about the need to do it.

If we rely upon the appropriations process, there is a risk that it won't get appropriated. Does the law, as it is currently written then, compel the providers of telephone services to go ahead with the installation of the technology anyway?

Mr. FREEH. There is a provision which would permit a district judge to compel compliance, even in the absence of reimbursable funds, if a finding was made that it was reasonable under those circumstances to proceed, but it is a legal solution as opposed to a congressional solution.

Mr. McMILLAN. We don't need to create any more lawyers than we have to. OK, let's assume that that is going to be compelling on the providers, and I think that is probably true. They would then try to pass it on in terms of rate cases to their consumers, and in most cases would ultimately succeed after a lot more legal expense and the creation of more legal jobs out there.

Why don't we try to get—

Mr. MARKEY. Would the gentleman yield? Just so that the audience can understand that you take some considerable pride in being one of the very few nonlawyers on this subcommittee.

Mr. McMILLAN. I expect to carry that with me to my grave. I have got a lot of lawyers in my family. I better be careful.

Actually, I think it could be argued that all telephone users and a high proportion of our citizens are more or less equal beneficiaries. Or, as you put it, Mr. Director, this potentially saves lives, potentially our lives. If we take this 500 million bucks—and I don't

know how many, Mr. Metzger, maybe you can tell me how many telephone call numbers exist in the United States.

Mr. METZGER. How many call numbers?

Mr. McMILLAN. Yes.

Mr. METZGER. Direct dial numbers, you mean?

Mr. McMILLAN. Yes.

Mr. METZGER. I am not sure.

Mr. McMILLAN. We have 250 million people. The average size of a family is three. That is almost 100 million telephones there, not counting business phones. We are talking about distributing the cost, probably in excess of 150 million telephone bills, not by the number of stations they have, but whether or not they use the service. So if we amortize the cost of this thing over 10 years, we are talking 50 cents a year.

I think it is conceivable and I will submit to the consumers out there who may be watching that most of us would be willing to do that for this measure of crime protection. It could be set up as an excise tax for this particular purpose, an anticrime surcharge on the telephone bill that would amortize the cost of this as distributed in accordance with the way the bill is written, and would sunset when the job is done.

I would simply throw that out as a reasonable possibility I think is equitable, and ask if you have any particular reaction to it.

Mr. REILLY. There is an option that you may want to—that you may want to consider down the road in that in many of these cases, both at the State and Federal level, there are funds that are seized as a result of these successful wiretaps, and some of them are used to defray the costs of the investigation. But they are asset forfeiture funds that certainly could be considered as a source of paying.

Mr. McMILLAN. Every time we try to nail those funds down, however, we get into a battle between local law enforcement and Federal law enforcement about who did most of the work and so forth and so on. That is pretty big money in some cases, and—I don't know. That is a good suggestion.

Mr. REILLY. It is just an option down the road in terms of how to pay that—at least consider it.

Mr. McMILLAN. I like to nail things down in front in terms of how we are going to pay for something, and this seems to be a pretty reasonable way to do it.

Mr. FREEH. I think your suggestion is a very reasonable one. Also there is a distinct possibility that the \$500 million would not all be expended. We are looking at that, in our view, as the outside reasonable limit as far as we are currently concerned.

One point, Mr. McMillan, which you made before which I would like to get back to in terms of phasing in this type of access on a geographical basis, we now have documented cases, for instance, tracking gang members, very large and violent gangs coming, for instance, out of California, who send scouts ahead—Omaha, Nebraska—go into a town. These are 15-, 16-year-old kids who are provided with a couple hundred dollars and a firearm. They actually scout out the area in terms of their ability to begin selling drugs, to begin all the violent criminal activity which these cities, many of them in the Midwest, are just now having. So this kind of organized colonization would make a good argument against a

heavy commitment of resources, particularly scarce ones, into definitive geographical areas which would ignore the large majority of Americans in smaller cities and towns.

Mr. McMILLAN. And so these telephone scams can occur anywhere, and would be logical targets of this kind of this surveillance activity.

Mr. FREEH. Yes, as with terrorism.

Mr. McMILLAN. Yes. Have we dealt adequately with the issue of parity. In other words, you don't see any holes in this insofar as the future is concerned?

Mr. FREEH. Except for the ones that Mr. Boucher indicated and which we have discussed with the industry, the private networks, we are very comfortable and satisfied that the universe of our most dangerous criminals is captured in the legislation and will be for the foreseeable future.

Mr. McMILLAN. All right. I think that answers my questions. Thank you.

Mr. MARKEY. Great. The gentleman's time has expired. I just have one final question, and then we can move on to the second panel.

And to you, Mr. Metzger, the legislation as it is developing in another committee here on the House side talks about what the FCC should do with regard to law enforcement and with regard to the standards, technologically, which have to be established; and it goes on at length to lay out what the obligations of common carriers are.

Could you just clarify it for the subcommittee again, where the general obligations of common carriers are found? Are they found in Title XVIII of the criminal laws, Mr. Metzger?

Mr. METZGER. No, Mr. Chairman. They are in Title II of Title 47.

Mr. MARKEY. I just wanted to clarify that with regard to where the responsibility was for putting obligations on common carriers. I just lost my bearings there in the U.S. Code, and I wanted to make sure that I can properly tie—we didn't want to have to go to a wiretap in order to locate the origins of the law.

Do any of the other members have any concluding comments which they wish to make?

It seems to me from the comments made by the members of the subcommittee that there is a general support for the thrust of the legislation which is being considered before the committee today. There are some fine points here that will have to be worked out, without question, although the nub of the controversy, it seems to me, does revolve around the cost and who should bear the cost and over what duration those costs should continue to be borne, either by the common carrier or by the general taxpayer. Those issues have yet to be determined, and I think Mr. Freeh is quite correct in putting the burden upon this subcommittee and the Congress generally to make that determination.

I commend the FBI and the district attorneys for their close cooperation with the Congress in working on this legislation. We would like to see a speedy conclusion to the negotiations and passage of the legislation, and if we could work closely with you in the ensuing several weeks, we will try our best to put that legislation on the President's desk.

And let me conclude then by giving each one of you 1 minute to summarize what you want us to remember as we go through this process over the final weeks, and we will go in reverse order.

Mr. Metzger, we will give each one of you 1 minute. Please begin.

Mr. METZGER. Thank you, Mr. Chairman. I think my purpose in testifying today was to make it clear that the Commission stands ready to carry out the responsibilities that the Congress may give it in carrying out these important public interest considerations and sensitive issues of national policy. We look to the Congress for guidance in these areas, and we certainly will carry out faithfully, as we have in the past, any responsibilities you give to us; and I reiterate, as I think my chairman has previously, we remain ready to assist you in any way in providing technical assistance as you go forward with your deliberations on this legislation.

Mr. MARKEY. Thank you, Mr. Metzger, very much.

Mr. Reilly, your final words.

Mr. REILLY. Thank you, Mr. Chairman.

What I would like you to remember is that there are State and local prosecutors throughout this country that rely upon this valuable tool, and if we don't get Federal legislation that is going to correct the problem that we have, public safety is certainly going to be jeopardized throughout this country. So I urge to you act quickly. I urge you to pass this legislation.

The cost, I think the Director has addressed that. It certainly is a factor. But when you are dealing with public safety and lives, that should be factored in. I don't think any cost is too great and certainly the 500 million that is allocated or could be allocated or appropriated for this should be sufficient to be very well spent.

Mr. MARKEY. Thank you.

And Director Freeh.

Mr. FREEH. Yes. I just want to thank you, Chairman Markey, the other distinguished members of this committee, the other committees who have worked on this. We are really on the brink of a remarkable achievement here, consensus quickly arising, which is really the result of 4 very long years of difficult and compromising negotiations.

It just seems to me that it would be a great shame to have this opportunity pass without the final goal of having this bill and having it perhaps this term. I would hate to be at a hearing 5 or 6 years from now and be explaining to you or any other Member of Congress that we could not prevent a disaster because 4 years ago we couldn't agree on how we were going to finance what everybody agreed had to be done.

So I am deeply appreciative of you personally, the other members of the committee, for the attention that you have given this.

Mr. MARKEY. Thank you very much.

And, again, we want to work very closely with you over the next 4 or 5 weeks, try to bring this whole issue to closure. We thank you.

This concludes the testimony from the opening panel. We will take a brief 1-minute recess so that the panel can be reset for our second group of witnesses.

[Brief recess.]

Mr. MARKEY. We will reconvene the hearing and hear now from our very distinguished second panel. And we will begin with Roy Neel, who is the president and chief executive officer of the United States Telephone Association. We have had a long association with Mr. Neel, Deputy Chief of Staff to the President of the United States, as well as Chief of Staff to Al Gore when he was a U.S. Senator, and who worked with this subcommittee for many years on all of the issues that we are considering, not just today but across the full spectrum, telecommunications issues.

We welcome you back, Roy. Whenever you feel comfortable, please begin.

STATEMENTS OF ROY NEEL, PRESIDENT AND CHIEF EXECUTIVE OFFICER, UNITED STATES TELEPHONE ASSOCIATION; JERRY J. BERMAN, POLICY DIRECTOR, ELECTRONIC FRONTIER FOUNDATION, INC.; THOMAS WHEELER, PRESIDENT, CELLULAR TELECOMMUNICATIONS INDUSTRY ASSOCIATION; AND DANIEL L. BART, VICE PRESIDENT, TECHNICAL AND REGULATORY AFFAIRS, TELECOMMUNICATIONS INDUSTRY ASSOCIATION

Mr. NEEL. Thank you, Mr. Chairman. Sounds like I haven't been able to keep a job.

The first panel really did illuminate, especially with the subcommittee's help, the remaining principal issues in this legislation. It has come a long way. It has been a great example of how government and industry can work together to deal with a lot of these problems. But you can't escape this issue of cost.

Mr. Boucher was right on target in drawing out the questions that really are at play here; Mr. McMillan, the same way. You do face a terrible choice here—in fact, some real trade-offs. There is no free lunch in this—in this new environment.

Just a few months ago, in March, this subcommittee rewrote the rules by which this whole industry will play, and I would take some exception with Director Freeh's comment that the technologies that are not covered in this bill are infinitesimal, that they are not significant. In fact, this committee unleashed those new technologies to play a much larger role. So there is a significant issue of coverage here—not only the kinds of safe havens, like motel and hotels and certain kinds of office switching systems, but larger systems, such as what you referred to as CAPS, competitive access providers, who can wire whole neighborhoods or whole business districts. I suspect that the criminals that law enforcement is terribly concerned about, many will be sophisticated enough to figure out where those safe havens are.

Coverage is a very real issue, but just accept for a moment the Director's view that this is not a significant problem. You are still left with a terrible cost issue here. Our information all along has been that this \$500 million figure, while the GAO is correct, and others, that it is difficult to establish a real cost, that it is still terribly understated. Our estimates are that it will take as much as \$1.8 billion to solve the call forwarding problem—call forwarding service for wiretapping alone; and that is not insignificant.

It was good to hear law enforcement note that there have not been significant problems with wiretapping—the 180 or so in-

stances that the Director indicated dealt with the capacity issues of cellular, and they dealt with some other technical issues. He noted that I had mentioned that there are some circumstances which hamper or which can hamper law enforcement's ability to wiretap. But the fact is we have been working on those problems.

Just passing this legislation or creating a mandate—especially if it is an unfunded mandate—just passing this legislation will not solve those problems. Industry and government will continue to have to work together to solve these things. The suggestion that having a cutoff period of 4 or 5 years after which no reimbursement capability is allowed will somehow drive the industry to solve these problems quicker, will create inefficiencies, I think just turns the real situation on its head.

What you have done in legislation to stimulate investment in the information superhighway is to create an incentive to invest and develop all kinds of new products, all sorts of things that may be much more sophisticated even than speed dialing or call forwarding or whatnot, and sometimes it takes 4 or 5 years to develop those new services. There is no way to know what kinds of capabilities are going to be necessary 4, 6 years out. So it is not only arbitrary, it is penal to suggest that after 4, 5 or 6 years that law enforcement will no longer have to pay for what it is getting here.

The Director said that this is an important tool of law enforcement. That is absolutely correct and they need that to continue to have the ammunition flowing to attack these problems.

But the fact here is that the analogy was something like air bags and seat belts falls short. The consumer pays for an upgrade or safety device; the consumer gets the direct benefit. Here it is essentially a law enforcement benefit. Granted, it is good to society to have wiretapping capability. But the fact is here that law enforcement should be expected to pay for a service that it gets.

There is a terrible problem in simply deciding to fold this into the rate base. All of you on this subcommittee know the terrible problems you have in local communities, at the State level, in trying to get any kind of rate case approved with a new cost. So it is not quite that simple.

I would strongly encourage you to consider several things here. On the issue of coverage, consider what you have done earlier this year in creating a stimulus for new kinds of providers and decide whether they should all be included. Should this umbrella include all carriers and all potential providers and not simply the local exchange providers?

Consider whether this funding of this capability should be cut off after several years. You would face terrible problems in the courts. Remember, this is not just an issue for large telephone companies, whether it is Bell Atlantic or NYNEX or Southwestern. It is not just those companies. You all have small telephone companies in your own districts. These companies will come under this mandate in exactly the same way. It isn't the very largest carriers.

As the Director says, there is a reasonableness issue here, that we wouldn't expect a company to do something that is unreasonable. But the fact of the matter, the mandate is still there. When one of these companies, whether it has 10 million or 8 million subscribers, or whether it has 300 subscribers, they are facing terrible

penalties if they don't meet law enforcement's guidelines here with these switches.

There is no way to geographically carve out certain exchanges or to create an exemption, as we do with rural exemptions in a number of areas. You can't do that. That fundamentally undermines what law enforcement is trying to do. So you face a difficult choice here.

If you apply this to all telecommunications carriers, then you have got to face the responsibility of how they are going to be paid for meeting this law enforcement request. It is not just the big Bell Operating Companies. It is every little telephone company. And we have about 1,300 of them. So you can't forget that issue.

So I think the problems are solvable if you deal with the problems in the outyears. If you deal with the issues of coverage, you can fix this. It is also correct, as the first panel suggested, there is no disagreement whatsoever in policy here. We all want to support law enforcement's efforts to carry out these wiretaps. We know of no cases where local telephone carriers have frustrated the efforts directly to execute a wiretap.

District Attorney Reilly made the suggestion that these telephone companies won't provide a wiretap unless a court order is delivered. There was some suggestion of reluctance there. The fact is, we don't have a choice. You have to have a court order to get a wiretap. And I don't think that public policy should be changed to reflect anything else. I mean, law enforcement should get a court order.

So there has been great cooperation. There has also been great cooperation in the last couple of years to address these most compelling problems, call forwarding, speed dialing and those kinds of things. And it is not going to go away simply by passing this legislation, and someone is going to have to pay.

So just simply dealing with the realities of the marketplace that you are helping create now will go a long way to solving these problems. Thank you.

Mr. MARKEY. Thank you, Mr. Neel.

[The prepared statement of Roy Neel follows:]

Testimony of Roy Neel, President

**United States Telephone Association
on FBI Wiretap Legislation**

USTA represents more than 1,000 small, medium and large local exchange telephone carriers throughout the United States. We commend Chairman Ed Markey, members of the Telecommunications and Finance subcommittee, and subcommittee staff, particularly Gerry Waldron and Mike Regan, for their efforts in holding this hearing.

USTA has been an integral force in negotiations with industry, privacy organizations and law enforcement on this important legislation. We remain fully committed to working with Congress to develop a bill that will stand the test of time.

While this legislation is a considerable improvement over earlier versions, it remains biased against the public switched network; lacks sufficient protection against unreasonable government requirements; and imposes new cost burdens on the nation's telephone companies. As currently written, the bill may hinder investment in and deployment of new network services at a time when investment in the national information infrastructure is a matter of national policy.

Is This Legislation Necessary?

It is important to note that law enforcement authorities conduct about 1,000 wiretaps a year in the nation. Of those, roughly half are conducted in the New York City metropolitan area. About a quarter are cellular-based, and half of these occur in just two states.

The FBI has identified 183 "technology-based problems" which it claims have hindered law enforcement wiretap efforts. Fifty-four of those cases related to cellular port capacity available to perform wiretaps. The second largest group was "other." Only thirty cases out of thousands of wiretaps actually dealt with technology-based services such as call forwarding or speed dialing. Even so, we are not aware of any cases in which the FBI has been unable to perform wiretaps because of technological restrictions.

The New York Times reported on March 1, 1994, that documents obtained through the Freedom of Information Act indicated that a survey of several FBI offices found "no instances in recent years in which FBI agents had encountered any technology-based problems in conducting wiretaps." Indeed, where any difficulties have arisen they have been quickly and satisfactorily resolved. (See Digital Privacy and Security Working Group Interim Report, March, 1994, which outlines current law-activities in meeting law enforcement requirements.)

The area of greatest concern to law enforcement authorities is not in technological barriers to interception, but in capacity limitations in the wireless/cellular environment, where tremendous demand growth has limited the number of ports available to law enforcement for conducting wiretaps.

USTA's concerns with this legislation have these foci: 1) cost recovery; and, 2) scope of coverage, and the effects these provisions have on competition and the deployment of new telecommunications services and technologies.

Cost Reimbursement**Costs are Difficult to Estimate**

This bill contains \$500 million for the first four years following enactment to cover the government's costs for developing and deploying the modifications necessary to bring existing facilities into compliance with law enforcement requirements.

Communications Daily in an August 4, 1994, article, noted it had obtained the FBI's confidential cost/benefit analysis upon which the \$500 million figure is based. The analysis demonstrated several flaws. For example, the "FBI figures didn't include cost of upgrading or maintaining switch software and didn't account for new technologies, such as PCS. Nor did it factor in costs that cable companies would have to pay when they began to provide telephone services."

In its testimony earlier this year before the House and Senate Judiciary subcommittees, USTA noted that the estimated cost of effecting software changes for call forwarding alone could reach \$1.8 billion. One large USTA member has estimated that it would cost over \$200 million to modify only its existing call forwarding features to accommodate government requirements in this bill. BellSouth requested a vendor's "inquiry-level" estimate for complying with the FBI's requirements on its wireline business only. The estimate: \$138 million to \$247 million.

Government Accounting Office (GAO) Director of Information Management Resources, Hazel Edwards, testified before a joint House-Senate Judiciary Committee hearing on August 11:

"It is virtually impossible to precisely determine if \$500 million is adequate to cover the reimbursement costs of the provisions discussed in this bill because cost will depend on the evolving capacity requirements as well as on the yet-to-be-determined technical solutions... Industry cost estimates for land-line switch upgrades range from somewhere in the neighborhood of \$15,000 to upwards of \$100,000 per switch, depending, of course, on the extent of changes required in the hardware and software."

FBI Director, Louis Freeh, acknowledged this uncertainty during the same hearings when he stated, "I just think there is a very, very difficult block to fill with respect to estimating that cost."

In short, \$500 million, as far as we can tell, won't even come close to the mark. USTA's principal concern with this legislation, therefore, is what happens when, or if, the \$500 million fails to cover the costs of complying with the government's requirements. Are companies and consumers protected if the government fails to reimburse? Or can the government impose its requirements "invisibly" on industry regardless of cost or need?

"Goldplating"

The record for government cost reimbursement for existing law enforcement activities does not give cause for great comfort with industry members, either. One USTA member company, with only moderate law enforcement obligations, spends \$3.7 million a year accommodating over 100,000 law enforcement subpoenas, many of which require boxes of documentation.

These expenditures of time and personnel are borne by the companies alone, without government reimbursement, even though the companies frequently request compensation for their efforts.

One can only presume that these obligations are only a fraction of those imposed on such companies in which law enforcement activity is more concentrated.

And, perhaps because there is no mechanism that limits government's "free" access to any information it wants, its demands for customer information have been increasing dramatically on an annual basis.

In fact, in June of this year, at least one of USTA's large company members received a subpoena from the Drug Enforcement Agency requesting "the identity of published and unlisted residential and business telephones...by area code, and telephone number, together with first name, last name (company name), address, city and state for all published and unlisted residential and business telephones in the service area..."

Besides the sheer audacity of this request, as well as its obvious implications regarding privacy and security of innocent American citizens, there was naturally no offer to compensate the company for complying with the agency's demands, despite the fact that commercially available data bases (purged of non-published numbers) exist on the market today.

There must be a mechanism for preventing the government from making excessive demands, when a more modest and less expensive solution may satisfy most of the government's objectives.

Prioritization

During the August 11 joint hearings, FBI Director Freeh testified that

"...the wisest way to approach [cost] is to...address on a priority basis the things that need to be done...[W]e have a pretty good idea where, based on past crime patterns, the most likely venues and the most critical needs for capacity are. We do not propose, and I don't think anybody is proposing, to rewire America..."

This bill, however, provides no incentive to require the government to establish priorities, particularly in the period following four years after enactment. Because there is no obligation for the government to pay for what it demands, it can require American consumers essentially to pay for a Cadillac solution, when a Geo solution may accomplish most of its needs. Or, it can demand compliance, regardless of cost, in areas in which it knows there is or will be little or no need for surveillance capabilities. Why should either American consumers or taxpayers pay for surveillance capabilities that are neither desirable nor necessary in most American cities and towns?

This legislation must ensure that government establishes realistic priorities in determining where, when and how to deploy surveillance capabilities, not just in the first four years but as long as the act remains operative.

Ubiquitous Compliance

USTA strongly objects to the notion of mandating ubiquitous, national compliance with the requirements of this act, especially if this is achieved at the expense of American consumers.

Mandated ubiquitous compliance disregards important consideration of either the need or cost-effectiveness of compliance by relieving the government from the obligation to prioritize its requirements or to determine where and how to find cost-effective solutions to its law enforcement goals.

And, to the extent that such costs are significant - and we have every reason to believe they are - then what effect will a ubiquitous compliance mandate have on the deployment of new features and services in rural America, or on companies less able than others to pay?

As USTA noted in testimony earlier this year, a poll conducted by Yankelovich Partners in March and reported in Time Magazine found that "two-thirds of Americans said that it was more important to protect privacy of phone calls than to preserve the ability of the police to conduct wiretaps."

As FBI Director Freeh testified on August 11, "We have exempted...a fairly significant segment of the evolving telecommunications industry" from coverage under this legislation. Thus, it appears that the FBI has already considered and rejected the notion of ubiquitous compliance requirements.

The Opportunity Costs of Surveillance Requirements

It should be noted that whatever the costs of compliance, they represent time, effort, investment and resources to meet government demands that could otherwise be devoted to productive alternatives.

To the extent that government fails to reimburse providers for such time and investment that is dedicated to meeting law enforcement's surveillance demands, and not developing advances in network enhancements for the improvement of private and commercial communications capabilities, then this Act has to be measured in terms of its opportunity costs; i.e., resources lost or diverted from other pursuits.

"De Minimis" Costs After Four Years

It is not reasonable to assume that costs will, as claimed by the FBI, be merely "de minimis" after four years.

Costs associated with developing and deploying new features simply are not "de minimis." As with the development of any feature, it takes time and money to meet additional requirements, particularly requirements as complex as those being posed by the FBI. The costs of such "low-tech" features as passenger air bags in automobiles is very high even today, and with these there is a high consumer willingness to pay. Even so, no one is proposing to pay for air bags for every seat. The costs of such "ubiquitous coverage" are prohibitive, despite the technology having been available for years and deployment having been incorporated into the design of cars.

What if the government's assumption about de minimis costs proves wrong? Since the government is the sole customer for the requirements it imposes, then it should bear the risk of assuming the cost burden.

A Surveillance Budget

If it is only for the first four years that the government is given its \$500 million authorization, then nothing in the bill

prevents the government from asking a company in the fifth year after enactment to modify its facilities to comply with the Act's requirements.

This legislation should clarify that the government cannot come back to a company in the fifth year, or later, and demand compliance for that which it could not afford, or did not properly plan for during the first four years.

What is needed is a means to prevent government from making unlimited demands at the expense of privacy protection and American consumers. In short, government needs cost containment incentives.

This can be accomplished by strictly limiting law enforcement demands to those capabilities for which it can pay. The requirements of the Act should not apply to telecommunications providers, equipment, features, or services for which the government fails to provide reimbursement.

The \$500 million authorized for the government's implementation of the Act thereby would become a "surveillance budget" under which law enforcement would be forced to develop appropriate priorities and reasonable requirements. If, in fact, the government's estimated cost of compliance is \$500 million, then it should be able to accomplish all of its objectives within this budget. If, however, \$500 million is too small an amount, then the government will need to determine where and how to best spend its surveillance budget.

Further, if the costs of compliance after four years following enactment are truly de minimis, as the government claims, then its costs will also be minimal.

The Government Should Pay for What it Gets

The government normally pays for goods and services it procures. For instance, airplanes, tanks, and other national security materiel is designed, developed, and manufactured for government-specific requirements and, in turn, paid for by the government. Secure telecommunications systems, satellite systems, custom automobiles, bullet proof vests, and even pencils are acquired and costs reimbursed.

Any uncertainty with regard to whether companies will be reimbursed for their costs of compliance will necessarily hinder their willingness and ability to deploy new services. The effects of this uncertainty will be exaggerated in rural areas and/or other areas where providers are less able to afford costs of compliance.

Thus, government must have an obligation to determine what it wants and how much it is willing to pay -- including for regular network or feature upgrades. Companies must be able to deploy new services in a timely manner with certainty that either they will be reimbursed, or they will be protected if government fails to reimburse them.

Benefits of Government Reimbursement

There are several advantages to requiring the government to pay for what it gets. Most importantly, it maintains incentives to invest in and deploy new telecommunications services and technologies by 1) providing certainty to companies that they may deploy new services and not suffer additional costs or possible court proceedings; and 2) not diverting investment from services to compliance.

A surveillance budget forces the government to establish priorities. While it may want ubiquitous national compliance with Cadillac surveillance technologies, limiting government requirements only to what the government can pay for prevents it from such "goldplating." Lack of any reimbursement requirement would give the government no incentive to contain its costs, and would establish an unfunded mandate for consumers to pay the tab for government surveillance. Law enforcement will have to concentrate on what solutions are most cost effective and where its expenditures are needed most, rather than to ask for ubiquitous capability deployment where there may be little or no need. The government would need either to limit its spending requests or modify its technical requirements.

Government reimbursement ensures that government surveillance expenditures remain in the "sunshine," subject to public scrutiny. Without an obligation to reimburse costs, the government could "hide" its requirements, and the public would absorb costs of compliance without knowing how much is being spent in complying with the Act. Not only would American consumers be paying directly for the government's invisible surveillance requirements, but they would be paying in lost investment, as noted above.

Competitive neutrality is maintained under a government reimbursement requirement. Particularly since not all providers or telecommunications networks are treated equally under this legislation, companies covered by the Act would not be forced to incur costs (at a competitive disadvantage) that other companies do not face. This becomes even more problematic in the changing regulatory environment facing telephone companies today. The introduction of competition into telecommunications markets undermines a carrier's ability to recover non-market costs - such as surveillance costs - from its customers.

Reimbursement protects small companies and others which will be disproportionately affected by the costs of complying with this Act. Most USTA members can ill-afford million dollar fixes (that may be considered under the Act as "reasonable") for building capabilities that may never be used.

It should be noted that the legislation already provides reimbursement, in perpetuity, for compliance with capacity requirements. Such reimbursement simply should be extended to compliance with the Act's capability requirements as well.

Reimbursement Procedures

This bill contains a provision granting the Attorney General authority "to establish any procedures and regulations deemed necessary to effectuate timely and cost-efficient reimbursement..." At least two USTA member companies are victims of non-payment of long-outstanding bills.

USTA recommends adding language to this provision that ensures a process by which industry has an opportunity to effect these regulations, and that requires issuance of such regulations in a timely manner.

The Australia Example

With the introduction in 1991 of competition in its telecommunications market, the Australian government granted to carriers the right to charge for assistance they provide to police authorities.

The government's decision was based on the following factors:

1. When Telecom Australia was a government monopoly, charging for surveillance meant the government in effect was charging itself for surveillance costs.
2. With the introduction of competition, the government considered it unfair to the shareholders of those companies that they should bear the costs of government requirements.
3. Because of the size discrepancy between Telecom Australia and the new entrants, the government also considered it unfair to impose a higher relative cost on smaller companies.
4. The government determined costs should be visible to the public so that an assessment can be made about whether the costs of a particular service or facility are worth the benefits derived from those services or facilities.
5. Police authorities had been accused of having no incentive for efficiency or cost containment.

The Minister of Communications recently concluded a review the government reimbursement mandate. The review reaffirms the basic principles outlined above that the costs of intercept facilities should be borne by the taxpayers.

Scope and the Issue of Competitive Neutrality

Legislation Covers Only a Portion of Telecommunications Traffic

In joint Judiciary Committee hearings on August 11, USTA President Roy Neel claimed that this legislation creates a "safe haven for criminals" by effectively creating two separate kinds of telephone networks: those covered by the bill, and those not covered.

During the same hearings, FBI director Freeh was asked by Senator Leahy whether "there are going to be areas you are not going to be covering." "That is correct," Director Freeh answered, but "that doesn't mean that we give up the whole universe of opportunity."

The fact is this legislation intentionally excludes significant portions of the telecommunications market from having to comply with law enforcement surveillance requirements. Networks such as the seven office buildings of the World Trade Center, the state of Iowa, the University of Michigan, hotels, airports, office campuses, and a host of other "private" telecommunications networks are excluded from coverage under this bill.

These telecommunications networks often dwarf the size of most USTA members. Moreover, they have the luxury of focusing their activities on the most profitable portions of telecommunications traffic - high volume, high margin business users.

Thus, as Director Freeh said at the same hearing, "There is a part of the sophisticated criminal world which will not be captured in this bill." But is that sound public policy?

It would seem reasonable that law enforcement agencies would wish to consider "the whole universe of opportunity" when determining where to place surveillance capabilities. If not, then we are indeed creating a safe haven for "sophisticated" criminals.

It appears that law enforcement accepts the notion of having a dual telecommunications infrastructure: one--the public switched network, with "built-in" surveillance capabilities--and the other, a secure "private" network. If this is government policy, then the issue of ubiquitous deployment is moot. All the money spent by this Act will have been wasted, as users simply find a way to divert their traffic to the alternative, secure network.

To the extent that one group of telecommunications providers has to develop and deploy surveillance capabilities for its networks while a significant portion of alternative providers does not, then an artificially mandated marketing advantage is created for the latter. Businesses and consumers interested in enhanced security - a major marketing and customer loyalty factor in winning and retaining consumers - will opt for "private" networks.

And since not all companies are covered evenly by the legislation, separate equipment markets will emerge to provide feature specific solutions for customers. Most switches are built and installed outside of the U.S.; there already exists a large source of equipment which will not need to be built to U.S. law enforcement specifications.

The ability to conduct wiretaps in the old days was an accident. "State of the art" technology was as easy to tap as buying a pair of alligator clips and hooking them to a telephone line. Nowadays, it is not that easy. And it is expensive. There is a vast variety of technologies and services being offered by a panoply of companies often serving the same customer with similar or even identical services.

As a matter of sound public policy, these services and technologies should be included under the coverage of this bill. However, as a matter of practicality, it is unreasonable to expect either the American taxpayer or consumer to foot the bill for universal, ubiquitous surveillance capability deployment.

Consequently, the cost provisions of this legislation are directly related to the scope of coverage. That is, the government must be required to reimburse telecommunications providers covered by the bill for the expenses they incur in complying with government requirements. If they are not reimbursed, the requirements should not apply.

Otherwise, if some companies are required to comply and foot the bill themselves, and other companies are not, a significant competitive disadvantage would be imposed on the former. Moreover, nothing would prevent the government from imposing requirements ubiquitously and at any expense, regardless of cost or need for such capabilities.

However, with a permanent reimbursement requirement, and with coverage of all telecommunications services, rather than a certain class of companies, the government would need to determine where, when, and how to spend its limited resources. Companies would know that they would be "made whole" (i.e. they would not be competitively affected by the bill) by government reimbursement. And American consumers would know that government

surveillance is subject to a budget, which in turn is subject to public scrutiny.

Legislation Should Cover Services, not "Entities"

USTA has continually proposed language which would apply the requirements of the Act evenly to any service which involves switching or transmission of electronic communications for hire to unaffiliated parties. By applying the bill to services, and not to companies (i.e. common carriers), the bill would attain competitive neutrality.

The Sectional Summary accompanying this bill includes a reference to a functional definition of "local exchange carrier" in House-passed H.R. 3626. This support language should be put into the legislative language.

The legislation does provide the FCC with authority to determine when or if an alternative service provider should be covered by the bill "when such service is a replacement for a **substantial portion** of the local exchange service and that it is in the public interest to deem such person or entity to be a common carrier for purposes of this Act." (Emphasis added.)

But clearly, there is already difference of opinion in interpreting "substantial portion" since many of the aforementioned networks are not covered.

Reasonableness and Deployment of New Services and Technologies

Senator Leahy is quoted in the August 10 edition of Communications Daily as saying that the goal of this legislation "is to assist law enforcement needs without...frustrating the development of new communications technologies or the competitiveness of America's high-tech industry."

Companies must be able to deploy new services in a timely manner with certainty that either they will be reimbursed for their costs or compliance, or they will be protected if government fails to reimburse them. No one wants to end up in court or in other protracted legal proceedings to determine if and whether their expenses are reimbursable or whether equipment or features can be deployed without threat of eventual withdrawal from the market.

FBI Director Freeh's comments on August 11 were encouraging in this regard. He noted that if telecommunications providers "are unable to achieve a certain agreed-upon standard, either because of technological problems or funding problems, they are protected."

But reasonable minds are still debating whether the actual provisions of this legislation provide the comfort level necessary to allow companies to make the investment decisions to deploy new services and features. Doubts still exist as to whether companies can deploy technology that cannot currently be tapped without facing the threat of court action and possible withdrawal of a technology, service or feature.

If a company is faced with investing millions of dollars in a new product but finds in the middle of its development efforts that a surveillance capability will be very difficult - and expensive - to develop, the company may decide to "cut its losses" and abandon an otherwise valuable product development effort.

Further, if a technology is achievable, the bill requires that companies comply with the capabilities requirements. Does this mean that a small telephone cooperative in rural Vermont must modify or retrofit its facilities even though there is little or no likelihood that its surveillance capabilities will ever be needed?

For example, the FBI's REQUIREMENTS document declares law enforcement's desire to "follow" calls through the network to their ultimate destination. This may be possible as an application of advanced intelligent network (AIN) technology, not yet deployed. One conservative estimate of the cost of deploying this feature would be \$100 million per region. To support the FBI's requirements, AIN would need to be deployed universally, which is not currently being contemplated.

To satisfy these lingering doubts, the bill must provide a reasonableness standard and not guarantee absolute compliance with law enforcement's requirements. Good faith efforts to comply should be sufficient to find a company in compliance with the Act.

In this regard, it must include **economic feasibility** as well as **law enforcement needs** in determining compliance. The Sectional Summary accompanying the bill includes a discussion of economic reasonableness in describing the bill's intent. This language needs to be placed in the legislation itself.

The relative costs and benefits of the bill's requirements placed on all companies must also be a factor in determining compliance. Otherwise, ubiquitous deployment of all "publicly available" capabilities would appear to be required by the bill.

Reasonableness and Timely Action

The Act states that companies must comply with the capabilities requirements only if "(i) alternative technologies or capabilities or the facilities of another carrier are not reasonably available...and (ii) compliance with the requirements of this chapter is **reasonably achievable** through the application of available technology...or would have been achievable if **timely action** had been taken." (Emphasis added.)

The term "reasonably achievable" leaves much to the imagination, especially without specific reference to economic feasibility or cost-effective deployment considerations. Moreover, what "timely action" should have been taken? There is simply too much ambiguity for determining whether this provision could permit a court to retroactively order a company to withdraw or ban deployment of services or technologies at some time in the future.

Both of these terms need clarification before any company will feel safe investing the considerable money and resources needed to deploy new technologies and services.

Responsibility of Manufacturers

USTA believes that the legislation now requires full cooperation and compliance of manufacturers with the requirements of the Act. Without shared responsibility, it would be possible for a carrier to face a court injunction against deploying a new technology or service when a manufacturer fails to provide it with the necessary capabilities which may be technologically or economically achievable, just not available.

USTA Recommends the Following Changes to this Legislation:

1. Cost

The government should reimburse telecommunications providers for all reasonable costs of compliance, regardless of when they are incurred. Compliance requirements must not apply to companies, features, services, etc. for which the government fails to provide reimbursement. Government should prioritize its demands, limit compliance to where it is needed most and what solutions are most cost effective.

2. Scope:

The bill should cover all telecommunications services, rather than "carriers." Reference to a functional definition of "local exchange carriers" in House-passed H.R. 3636 is given in the Sectional Summary accompanying the bill. This definition should be made part of the legislative language. Any transmission or switching of electronic communications to unaffiliated parties for hire is a telecommunications service.

3. Reasonableness:

Ensure that good faith efforts to comply with the requirements of the Act are sufficient grounds for compliance. Eliminate any doubt as to whether companies can invest in and deploy new upgrades, services or technologies without fear of delay, additional unfunded government mandated costs, or protracted court or legal proceedings.

Put into the legislative language the Sectional Summary discussion of economically feasibility as a criterion of compliance.

Conclusion

Telephone exchange companies will, as they have consistently in the past, endeavor in good faith to meet the requirements of the law enforcement community.

It is important to remember that there are about 1,000 wiretaps performed each year in the United States. The government intends to spend about \$125,000 per wiretap per year for the next four years, if it sticks to its budget.

While industry is willing to facilitate the objectives of law enforcement whenever feasible, we cannot afford to raise barriers to investment in and development of new telecommunications technologies and services.

I thank the committee for allowing USTA to testify. I look forward to continuing the process of improving this Act so that it can maintain current rates of investment in our national information infrastructure while satisfying the objectives of our nation's law enforcement community.

Mr. MARKEY. Our second witness, Mr. Jerry Berman, is the policy director for the Electronic Frontier Foundation, a very good friend of this subcommittee.

We welcome you back, Jerry. Whenever you are ready, please begin.

STATEMENT OF JERRY J. BERMAN

Mr. BERMAN. I appreciate the opportunity to be here, Mr. Chairman, members of the committee, Representative Boucher. This is extraordinarily important legislation and it is very important and hopeful that this committee take a look at it, because you bring the expertise of understanding our telecommunications system and the deployment of technology.

We have wrestled, along with industry, to try and ensure that this legislation, if it was going to happen, did strike a balance between law enforcement needs and privacy and the fourth amendment. We have spent a great deal of time ensuring that there is no expansion of law enforcement authority to conduct wiretaps here. They get what they used to get pursuant to a court order.

We have ensured new privacy protections for transactional information, the rich amount of detail which is flowing through the telecommunications network and that will require a court order under this legislation. We have ruled out the ability to just track everyone using these advanced systems, so remote tracking has been ruled out. Citizens may still use encryption.

And, finally, in all of this process to decide what these requirements are, privacy advocates can intervene and privacy is a consideration in the process.

But really we think that keeping this balance and ensuring that it is implemented with a balance between law enforcement and privacy requires that we address these issues of costs. We think that it is very important to resolve the question of who bears the risk and who bears the burden of paying for costs, not only in the first 4 years.

The assumption of the legislation is that somehow the first 4 years, \$500 million will take care of it. We are concerned about, what if the \$500 million isn't enough, and certainly in the outyears, whether in fact the costs are more than de minimis. The government assumes they are de minimis. We think they might be substantial.

We think that the best way to resolve that dilemma is to make the costs borne by the government simply because if they are de minimis, then the government won't—the taxpayer wouldn't be paying a lot of money. If they are substantial, those costs will be on the table; they will be above board and we can have public accountability.

This legislation is taking us off in a new area where the FBI is setting some standards for our telecommunications system. So be it. But it ought to happen in the light of day, the clear light of day. We want to make sure that there is no shortchanging of privacy, either by industry, when there is not enough money being made available, taking shortcuts to solve law enforcement problems in trying to meet the requirements of this legislation.

We also want to make sure that the government prioritizes its law enforcement needs and doesn't create new problems that are unnecessary, that it doesn't create new security problems which are unnecessary and we shouldn't bear as a public.

We want to make sure innovation can go forward. One of the key parts of this legislation assures that industry can deploy new services which even may be untappable or may be difficult to tap, but this legislation must also remove the chill of innovation not going forward because it might cost too much to meet the FBI's requirements. You want to remove that chill, make the government responsible for paying the reasonable cost of the upgrade in order to make that service meet their standards.

And, finally, it is just a matter of public accountability. We want to know how our law enforcement dollars are spent. We want to know whether money that is being diverted from law enforcement should be going to other public goods—privacy, building of the information superhighway. The answer to that is that we ought to cover costs in the near term and in the long term, and we urge amendment to the bill to make that clear.

Thank you.

Mr. MARKEY. Thank you, Mr. Berman, very much.

[The prepared statement of Jerry J. Berman follows:]

Statement of Jerry J. Berman, Policy Director, Electronic Frontier Foundation

Chairman Markey and Members of the Subcommittee:

I want to thank you for the opportunity to testify today on the recently introduced Digital Telephony bill (H.R. 4922, S. 2375). Over the past several years under the leadership of Chairman Markey, Representatives Fields, Boucher, and others, the Subcommittee has demonstrated knowledge, sensitivity, and vision in crafting our nation's telecommunications policy. I am pleased that the Subcommittee has chosen to apply its experience and expertise to the extraordinarily complex issues posed by the Digital Telephony legislation.

The Electronic Frontier Foundation (EFF) is a public interest membership organization dedicated to achieving the democratic potential of new communications and computer technology and works to protect civil liberties in new digital environments. EFF also coordinates the Digital Privacy and Security Working Group (DPSWG), a coalition of more than 50 computer, communications, and public interest organizations and associations working on communications privacy issues. I am testifying today, however, only on behalf of EFF.

Since 1992, the Electronic Frontier Foundation has opposed a series of FBI Digital Telephony proposals, each of which would have forced communications companies to install wiretap capability into every communications network. However, earlier this year, when it became apparent that some version of the bill would pass the Congress, Senator Patrick Leahy and Representative Don Edwards asked EFF, along with computer and communications industry groups, to participate in a process that would yield a narrow bill that both met law enforcement needs and had strong privacy protections. The result of that process is the bill before us today.

EFF remains deeply troubled by the prospect of the federal government requiring communications networks to be made "wiretap ready," but we believe that this legislation is substantially less intrusive than the original FBI proposals. If Congress is going to act in this area, it should work to improve and pass this version of the legislation.

As I testified to before a joint hearing of the House Subcommittee on Civil and Constitutional Rights and the Senate Subcommittee on Technology and

the Law on August 11, 1994, we have worked diligently on this legislation with all interested parties in an effort to strike a careful balance between law enforcement's ability to conduct electronic surveillance and the more important public good -- the right to privacy guaranteed by the 4th amendment. The bill strikes this balance in a number of critical areas:

- Law enforcement gains no additional authority to conduct electronic surveillance. The warrant requirements specified under current law remain unchanged
- The standard for law enforcement access to online transactional records is raised to require a court order instead of a mere subpoena
- Information gleaned from pen register devices is limited to dialed number information only. Law enforcement may not receive location specific information
- The bill does not preclude a citizen's right to use encryption
- Privacy must be maintained in making new technologies conform to the requirements of the bill and privacy groups may intervene in the administrative standard setting process.

However, Mr. Chairman, the effectiveness of these privacy protections, as well as the future of technological innovation and the deployment of advanced telecommunications services to the American public, turn on one critical issue which remains to be addressed: Who assumes the risk and pays the cost of complying with the bill's requirements? The government or industry?

EFF believes that allocating the risk and cost to industry will place privacy and security at risk if industry is required to foot the bill for unnecessary or unwarranted surveillance capabilities. Similarly, privacy may be shortchanged if industry takes short cuts to save costs in meeting the legislation's requirements. Industry may also be discouraged from deploying new and innovative technologies because of the costs of law enforcement compliance features. Finally, public accountability is undermined by making potentially significant law enforcement costs without public scrutiny and debate. In our view, the public interest can only be served if government assumes the risk and pays the costs of compliance. While effective law enforcement may be in the public interest, it should not come at the expense of other public goods -- privacy, public accountability, and technological innovation. To resolve this issue, we believe that the legislation should be amended to require government to pay all reasonable costs incurred to meet the statute's requirements on an ongoing basis.

A. Linkage of cost to compliance requirements in the first four years – the FBI gets what it pays for and no more

The bill authorizes, but does not appropriate, \$500 million to be spent by the government in reimbursing telecommunications carriers for bringing their networks into compliance with the bill within the first four years of enactment. The FBI maintains that this is enough money to cover all reasonable expenses of retrofitting. The industry, however, has consistently maintained that the costs are five to ten times higher. Given the FBI's confidence in their cost estimate, we believe that telecommunications carriers should only be required to comply to the extent that they have been reimbursed.

In his testimony before a joint hearing of the House Subcommittee on Civil and Constitutional Rights and the Senate Subcommittee on Technology and the Law on August 11, 1994, the FBI director stated that "I think it would be [...] extremely unlikely for a district court judge in the process which is contemplated by this legislation to force compliance or use of any sanctions when compliance is impossible because of the non-reimbursement which is the predicate in the legislation". Based on the Director's previous testimony and other discussions with the FBI, EFF believes that the bill should include a provision to directly link telecommunications carriers liability with government reimbursement for retrofitting.

B. Government reimbursement for compliance costs after four years – public accountability necessary

The problem, Mr. Chairman, is that under the current bill, the government is not responsible for paying the cost of meeting the mandated capability requirements after four years, particularly with respect to new services. The FBI has repeatedly argued that the costs for incorporating surveillance capabilities in new services at the design stage will be *de minimis*, a contention which most industry representatives and EFF believe may not be correct.

As this Subcommittee is aware, it is impossible to estimate compliance costs for technologies which are not even on the drawing boards. The way to resolve the issue is to have the government assume the risks.

If costs for compliance after four years are truly *de minimis*, then the expenses born by the taxpayers will be minimal. If, however, costs are substantial, the government should pay. This will insure that the government,

on a case-by-case basis and with an opportunity for public oversight, determines if compliance is significant enough to pay for out of taxpayers' funds. This will also ensure that the government sets law enforcement priorities.

As I stated earlier, if the telecommunications industry is responsible for all future compliance costs, it may be forced to accept solutions which short-cut the privacy and security of telecommunications networks, or forced to leave advanced features on the shelf, slowing technological innovation and the development of the NII. Linking compliance to government reimbursement in the out years also has the added benefit of providing public oversight and accountability for law enforcement surveillance capability.

The drafters of this legislation have wisely included public oversight of government surveillance expenditures in the first four years. This same principal should be applied to out year compliance costs.

C. Ensure the right to deploy untappable services

The enforcement provisions of the bill suggest, but do not state explicitly, that services which are untappable may be deployed. Having worked for many years towards the goal of promoting the development of the NII, the members of this Subcommittee are clearly aware that its promise and potential rest on the deployment of advanced technologies and services. EFF remains deeply concerned that technological innovation and the deployment of advanced telecommunications services to the public may be stifled if telecommunications carriers are forced to incur huge costs for compliance, or if the Government is allowed to prohibit a new feature or service from being deployed. Although EFF believes that the bill intends to allow carriers to deploy untappable features or services, the bill must clearly state that if it is technically and economically unreasonable to make a service tappable, or if the government has failed to reimburse a carrier for compliance costs, then it may be deployed, without interference by a court. Making the government responsible for all reasonable costs of having new services comply with the legislation will go a long way to insuring that this legislation will not be a drag on innovation.

D. Additional areas where strengthening is necessary

In addition to our concerns about compliance costs, EFF believes that the bill requires strengthening in the following areas before final passage:

1. Strengthened public process

In the first four years of the bill's implementation, most of the requests that law enforcement makes to carriers are required to be recorded in the public record. However, additional demands for compliance after that time are only required to be made by written notice to the carrier. To facilitate public scrutiny, the bill should require all compliance requirements, whether initial requests or subsequent modification, must be recorded in the Federal Register.

2. Clarify definition of call identifying information

The definition of call identifying information in the bill is too broad. Whether intentionally or not, the term now covers network signaling information of networks which are beyond the scope of the bill. As drafted the definition would appear to require telecommunications carriers to deliver not only the signaling information generated by their own services, but also the signaling information generated by information services and electronic communication services that travel over the facilities of the telecommunication carrier. In many cases this may be technically impractical. Moreover, it is contrary to the policy adopted by the bill to maintain a narrow scope.

3. Review of minimization requirements in view of commingled communications

The bill implicitly contemplates that law enforcement, in some cases, will intercept large bundles of communications, some of which are from subscribers who are not subject of wiretap orders. For example, when tapping a single individual whose calls are handled by a PBX, law enforcement may sweep in calls of other individuals as well. Currently the Constitution and Title III requires "minimization" procedures in all wiretaps, to minimize the intrusion on the privacy of conversations not covered by a court's wiretap order. In the world of 1968, when the original Wiretap Act was passed, most subscribers telecommunications facilities carried single conversations on single lines. But today, many conversations are co-mingled on one broadband communications facility. In order to ensure that constitutionally-mandated minimization is maintained, the bill should recognize that stronger minimization procedures may be required.

E. New privacy protections

The Digital Telephony legislation before us includes significant recognition that new communication technologies, and new patterns of technology use, require new privacy protections. Thanks to the work of Senator Leahy and Representative Edwards and Senator Biden, the bill contains a number of significant privacy advances, including enhanced protection for the detailed transactional information records generated by online information services, email systems, and the Internet. These protections should remain in the legislation.

1. Expanded protection for transactional records sought by law enforcement

Chief among these new protections is an enhanced protection for transactional records from indiscriminate law enforcement access. For purposes of maintenance and billing, most online communication and information systems create detailed records of users' communication activities as well as lists of the information that they have accessed. Provisions in the bill recognize that this transactional information created by new digital communications systems is extremely sensitive and deserves a high degree of protection from casual law enforcement access which is currently possible without any independent judicial supervision.

EFF commends the authors of this legislation for recognizing that law enforcement access to transactional records in online communication systems (everything from the Internet to America OnLine to hobbyist BBSs) threatens privacy rights. Indiscriminate access to transactional records implicates privacy interests because:

- the records are personally identifiable,
- they reveal the content of people's communications, and,
- the compilation of such records makes it easy for law enforcement to create a detailed picture of people's lives online.

Based on this recognition, the draft bill contains the following provisions:

- **Court order required for access to transactional records instead of mere subpoena**

In order to gain access to transactional records, such as a list of to whom a

subject sent email, which online discussion group one subscribes to, or which movies a subject requested on a pay-per view channel, law enforcement will have to prove to a court, by the showing of "specific and articulable facts" that the records requested are relevant to an ongoing criminal investigation. This means that the government may not request volumes of transactional records merely to see what it can find through traffic analysis. Rather, law enforcement will have to prove to a court that it has reason to believe that it will find specific information relevant to an ongoing criminal investigation in the records it requests.

With these provisions, we have achieved for all online systems a significantly greater level of protection than exists today for records such as email logs, and greater protection than currently exists for telephone toll records. The lists of telephone calls that are kept by local and long distance phone companies are available to law enforcement without any judicial intervention at all. Law enforcement gains access to hundreds of thousands of such telephone records each year, without a warrant and without even notice to the citizens involved. Court order protection will make it much more difficult for law enforcement to go on "fishing expeditions" through online transactional records, hoping to find evidence of a crime by accident. We have also submitted a detailed memorandum on the importance of protection and would ask that this document be included in the record of these proceedings along with this testimony.

- **Standard of proof much greater than for telephone toll records, but below that for content**

The most important change that these new provisions offer is that law enforcement will: (a) have to convince a judge that there is reason to look at a particular set of records, and; (b) have to expend the time and energy necessary to have a United States Attorney or District Attorney actually present a case before a court. However, the burden of proof to be met by the government in such a proceeding is lower than required for access to the content of a communication.

2. New protection for location-specific information available in cellular, PCS and other advanced networks

Much of the electronic surveillance conducted by law enforcement today involves gathering telephone dialing information through a device known as a pen register. Authority to attach pen registers is obtained merely by asserting that the information would be relevant to a criminal investigation. Under current law, courts must approve pen register requests without any substantive review of the basis for law enforcement's request. This legislation offers significant new limits on the use of pen register data.

Under this bill, when law enforcement seeks pen register information from a telecommunications carrier, the carrier is forbidden to deliver to law enforcement any information which would disclose the location or movement of the calling or called party. Cellular phone networks, PCS systems, and so-called "follow-me" services all store location information in their networks. This new limitation is a major safeguard which will prevent law enforcement from casually using mobile and intelligent communications services as nation-wide tracking systems.

3. New limitations on "pen register" authority

Contemporary uses of pen registers also involve substantial privacy invasion, even aside from location information. Currently, law enforcement is able to use pen registers to capture not only the telephone number dialed, but also any other touch-tone digits dialed which reflect the user's interaction with an automated information service on the other end of the line, such as an automatic banking system or a voice-mail password. If this bill is enacted, law enforcement would be required to use "technology reasonably available" to limit pen registers to the collection of calling number information only. We are aware that new pen register devices are now on the market which automatically screen out all dialed digits except for the actual telephone numbers. Just as this bill would require telecommunications carriers to deploy technology which facilitates taps, we believe that law enforcement should be required to deploy technology which shields users communications from unauthorized invasion.

3. Bill does not preclude use of encryption

Unlike previous Digital Telephony proposals, this bill places no obligation on telecommunication carriers to decipher encrypted messages, unless the carrier actually holds the key to the message as well.

4. Automated remote monitoring precluded

Law enforcement is specifically precluded from having automated, remote surveillance capability. Any court-ordered electronic surveillance must be initiated by an employee of the telecommunications carrier, upon request by law enforcement. Maintaining operational separation between law enforcement agents and communication networks is an important privacy safeguard.

5. Privacy considerations essential to development of new technology

One of the requirements that telecommunications carriers must meet to be in compliance with the Act is that the wiretap access methods adopted must protect the privacy and security of each user's communication. If this requirement is not met, anyone may petition the FCC to have the wiretap access service be modified so that network security is maintained. This requirement, just like those designed to serve law enforcement's needs, must be carefully implemented and monitored so that, the technology used to conduct wiretaps cannot also jeopardize the security of the network as a whole. If network-wide security problems arise because of wiretapping standards, then the standards should be overturned.

F. Improvements over previous Administration proposals

In addition to the privacy protections added to this bill, we also note that the surveillance requirements are not as far-reaching as the original FBI version. A number of procedural safeguards are added which seek to minimize the threatens to privacy, security, and innovation. Though the underlying premise of the Act is still cause for concern, these new limitations deserve attention:

1. Narrow Scope

The bill explicitly excludes Internet providers, email systems, BBSs, and other online services. Unlike the bills previously proposed by the FBI, this bill is limited to local and long distance telephone companies, cellular and PCS providers, and other common carriers.

2. Open process with public right of Intervention

The public will have access to information about the implementation of the Act, including open access to all standards adopted in compliance with the Act, the details of how much wiretap capacity the government demands, and a detailed accounting of all federal money paid to carriers for modifications to their networks. Privacy groups, industry interests, and anyone else has a statutory right under this bill to challenge implementation steps taken by law enforcement if they threaten privacy or impede technology advancement.

3. Technical requirements standards developed by Industry Instead of the Attorney General

All surveillance requirements are to be implemented according to standards developed by industry groups. The government is specifically precluded from forcing any particular technical standard, and all requirements are qualified by notions of economic and technical reasonableness.

4. Right to deploy untappable services

Unlike the original FBI proposal, this bill recognizes that there may be services which are untappable, even with Herculean effort to accommodate surveillance needs. We understand that the bill intends to allow untappable services to be deployed if redesign is not economically or technically feasible. These provisions, however, should be clarified.

G. Conclusion

In closing, I would like to thank Chairman Markey and members of the Subcommittee, as well as others who have worked so hard on this legislation. The Electronic Frontier Foundation looks forward to working with all of you as the bill moves through the legislative process.



Expanded Protection for Online Transactional Information

Electronic Frontier
Foundation, Inc.
1001 G Street, NW
Suite 950 East
Washington, DC 20001

Phone: (202) 347-5400
Fax: (202) 393-5509
Internet: eff@eff.org

Ways may some day be developed by which the Government, without removing papers from secret drawers, can reproduce them in court, and by which it will be enabled to expose to a jury the most intimate occurrences of the home.... Can it be that the Constitution affords no protection against such invasions of individual security?¹

I. Overview

A. Spirit of ECPA calls for expanded protection for network transactional information

In the eight years since the enactment of ECPA, society's patterns of using electronic communication technology have changed dramatically. Over twenty million people now have electronic mail addresses, numerous business, nonprofit and political groups conduct work over the Internet, and "cyberspace" has become a household world. Indeed, it is now commonplace to speak about "life online." Records of all of these activities -- who sends a message to whom, where a given communications device is located, which political party one contacts for information, and which online discussion group or virtual community one associates with -- are available both in real time and in stored form as part of the transactional information generated by advanced computer and communications networks. With increasing use of telecommunications, this transactional information reveals almost as much about our private lives as would be learned if someone literally followed us around on the street, watching our every move.

As the ECPA drafters recognized, "the law must advance with the technology to ensure the continued vitality of the Fourth Amendment."² Under current law, much of this transactional information may be available to law enforcement merely by subpoena which recites that the requested information is "relevant to an ongoing investigation."³ In response to dramatic changes in the way that people use electronic communication services, ECPA should be revised to reflect the increasingly sensitive nature of network transactional information

B. Proposal to protect network transactional information that is personally identifiable or that reveals the contents of the communication

As this memorandum will demonstrate, the scope and depth of personal, sensitive information available through network transactional records has increased dramatically since the 1986 law was passed. Thus, EFF believes that the requirements for law enforcement access to certain categories of transactional records should be increased from a mere subpoena, which can be issued without independent judicial scrutiny, to a court order, which would only

¹ *Olmstead v. United States*, 277 U.S. 438, 467 (1928) (Brandeis, J., dissenting) (cited in ECPA Senate Report).

² ECPA Senate Report, p.5

³ 18 USC 2703(d). As will be discussed below, the statutory distinction between contents and records is unclear, so that current scope of law enforcement access is not a matter of settled law.

be issued upon a finding by a detached and neutral magistrate. All transactional records which:

- contain personally identifiable information related to an electronic communications, or
- reveal the content of the electronic communication

should be accessible to law enforcement only with a court order.

II. Online transactional information contains extensive personally identifiable information and thus deserves greater protection than telephone toll records

A. Personally identifiable information in online transactional records

The bulk of email addresses in use today are unique to an individual user. Either the address reveals on its face the identity of the user, or a simple command can be issued to translate the address into the owner's name.

Email addresses are personally identifiable

jberman@eff.org belongs to Jerry Berman
whitfield.diffie@eng.sun.com belongs to Whitfield Diffie

Therefore, unlike telephone toll records, a transaction indicating that a message is sent to or received from a particular email address is almost always a definitive record of a communication by an identifiable person. [For a detailed description of email transactional records, see Appendix A] Whereas, toll records record only the fact that a given telephone instrument connects an another instrument, a record of an email sent or received will establish the identity of the communicating party with some certainty. Ownership of a telephone instruments may be well-established, but without access to the content of the telephone communication, there is no proof that any individual was actually using the phone coincident with a communication recorded in toll records. In practice, courts also agree that toll records fall short of disclosing identity of the calling parties.⁴

Some early email systems tied the email address to a particular computer or terminal, just as a telephone number is tied to a given telephone instrument. But today, someone who owns an email address can use it from virtually any computer in the world. Moreover, no one else can easily use another person's email address, since the ability to send and receive mail with an address is generally controlled by password or other security device. While it is, in some cases, possible to use someone else's email address, this practice will increasingly be considered a fraud on the receiver of the message and a theft of service from the owner of the email account. By contrast, no fraud is required to use someone else's telephone number, unless one fails to pay the charges associated with the call.

B. Transactional records reveal location of sender and recipient

Transactional information in new mobile communications services such as cellular network and Personal Communications Services (PCS) provide law enforcement with information about the location and travel of users. These services are designed in order to deliver calls and other communications to the subscriber, no matter where in the country he or she is. As a side effect of this

⁴ In *United States v. Anderson* (542 F.2d 423, 1976), the 7th Circuit found that "toll records could not be relied on to show the contents of calls nor the parties thereto; ... identification of places called ... did not reveal the identity of the recipient or the nature of the call..."

feature, the network generates trails of transactional information that pinpoint the users location at any time that the user has the device turned on. For example, when a cellular phone is set to "roam" from one territory to another, it signals the network each time it crosses into a new service area, so that calls can be delivered to that phone and so that proper billing connections are established.

Furthermore, transactional records from mobile communications services will also reveal the movement of an individual from place to place, in real time. As the target moves from one cell or service area to another, an electronic trace of the fact that a given geographical boundary line is crossed will be created. If law enforcement has access to such traces, it will be possible to determine not only the targets location, but also his or her direction of movement.

Such location specific information goes far beyond simple calling and called number information contemplated by Congress when it authorized access to transactional information without a warrant or other judicial scrutiny. Where a probable cause warrant has been issued, we do not contest law enforcement's right have access to such information, where technically feasible. However, we believe that it is contrary to the Fourth Amendment and to the policy framework established in the 1968 Act and ECPA, to allow access to this increasingly rich source of information based on subpoena authority alone.

C. Online transactional records deserve a greater degree of protection than telephone toll records

In contrast to telephone toll records, online transactional information may reveal the identity of the communicating parties, and even the precise location of the communicators. These attributes distinguish online transactional records from traditional telephone toll records and other records generally available to law enforcement under subpoena power.

III. Content of communication revealed by online transactional Information

In many instances, addressing information from online systems will reveal the content or subject of the electronic communication. As in the example below, messages are often directed to, or received from discussion groups on particular topics.

EMAIL MESSAGE	
FROM:	djw@eff.org (Danny Weitzner)
TO:	eff-crypto@eff.org, whitfield.diffie@sun.eng.com
RE:	crypto policy update
DATE:	July 29, 1994, 08:15:48
This week significant progress was made on the Clipper front, but slide continues on export control liberalization...	

This message would be sent to everyone who is a participant in this particular group. Discussion groups (such as eff-crypto) are similar to telephone conference calls, except that they may last for days, weeks, or years. [See Appendix A for discussion of online transactional records logs which reveal such information.]

Here again, email address records are dramatically more revealing than analogous telephone toll records. Telephone toll records might reveal the fact that the user of a particular telephone was connected to a conference call service, but would not indicate the subject of that conference. In the email example, above, the subject of the conference is embedded into the address line, along with other individual addressed. Furthermore, since the conference name is indistinguishable from an individual email address, there is no way to segregate such information out of the transactional record stream.

B. Freedom of association and assembly implicated by disclosure of personally identifiable information

Not only does the transactional log of such a discussion group reveal the contents of the discussion, but also, the names of the parties to the discussion are disclosed in the logs. This as an excerpt from an actual email log which records the progress of the above from the sender to all of the members of the online discussion group.

```
01 7/29 08:15:48 IIA12559: from=<djw@eff.org>, msgid=<199407291215.IIA12559@eff.org>
02 7/29 08:15:49 IIA12559: to="/usr/local/etc/cryptoarchiver" stat=Sent
03 7/29 08:15:50 IIA12559: to="/usr/local/etc/mail2list eff-crypto eff-crypto-explorer",
04 7/29 08:15:51 IIA12565: from=owner-eff-crypto, msgid=<199407291215.IIA12559@eff.org>
05 7/29 08:15:51 IIA12565: to=gnu@toad.com (John Gilmore), delay=00:00:01, stat=queued
06 7/29 08:15:51 IIA12565: to=mkapor@kei.com (Mitchell Kapor), delay=00:00:01, stat=queued
07 7/29 08:15:51 IIA12565: to=jberman@eff.org (Jerry Berman), delay=00:00:01, stat=queued
08 7/29 08:15:52 IIA12565: to=jseiger@eff.org (Jonah Seiger), delay=00:00:01, stat=queued
09 7/29 08:15:51 IIA12565: to=djw@eff.org (Danny Weitzner), delay=00:00:01, stat=queued
```

First, line 1 of the log reveals that a message was sent to the eff-crypto discussion group. Then, lines 5 through 9 reveal the identity of all of the recipients of that message, in other words, all of the participants in this particular group.

For those who associate and assemble online, these email logs are equivalent to membership lists deserving of constitutional privacy protection. Inasmuch as online transactional records reveal the identity of the parties who are engaged in the discussion, fundamental constitutional rights such as freedom of association and freedom of assembly are implicated by any disclosure to the government. Since NAACP v. Alabama ex rel. Patterson, 357 US 449 (1958), courts have agreed that threats to privacy of association constitute impermissible intrusion on First Amendment freedom of association and freedom of assembly. The NAACP case involved a challenge to a government action which would have compelled the NAACP to disclose its membership list to the State of Alabama. The Supreme Court found that:

Inviolability of privacy in group association may, in many circumstances, be indispensable to preservation of freedom of association. *Id.* at 462.

Inasmuch as online transactional records reveal such group association, they should be given a high level of protection from government intrusion. The transactional records of online conferences discussed above and is shown in Appendix A, clearly reveal association with particular groups.

IV. Quantity, Detail, and Ease of Analysis of transactional records require expanded protection

With the passage of ECPA, electronic mail messages were given the same degree of privacy protection as first class mail. Notwithstanding the analogy drawn in 1986, there are significant differences between email addressing logs and information which may be obtained under a mail cover.

A. Transactional logs of email contain significantly more information than available from a mail cover

• Automatic email transaction trail

Email systems create detailed transaction logs as a matter of course, whereas the postal service only keeps address logs if specifically required to do so by valid legal process. Thus, in the case of email surveillance, law enforcement may decide after the fact of a particular transmission, to seek access to transactional records.

- **Automatic attachment of return address information**

When using US Postal Service mail, the addition of a return address which identifies the sender is entirely optional and requires an affirmative step by the sender. In contrast, most email systems automatically append a return address to each electronic mail message, thus guarantying that anyone who examines the email log, will be able to identify both the sender and recipient.

- **Email co-mingles functions traditionally accomplished with voice, fax, paper mail, and even face-to-face communications**

Email communication is often a substitute for many other forms of communications. An email message can replace a fax, a voice telephone call, a short note sent through the US mail, and even face-to-face communication. Therefore access to logs of such communication is vastly more revealing than a log of any other single form of communication. Courts have recognized an increased privacy interest in co-mingled information as compared to the same information in disaggregated form.

B. Increased privacy interest in compilations

The volume and detailed nature of email transactions raise much more serious privacy concerns than do either toll records or mail cover logs. The Supreme Court and the US Congress have recognized that computerized compilations of information raise unique privacy concerns. Beginning with the Privacy Act of 1974, Congress has acknowledged that "computerized data banks ... present issues considerably more difficult than, and certainly very different from, a case involving the source records themselves."⁵ Later, in Whalen v. Roe, the Supreme Court found that "[t]he central storage and easy accessibility of computerized data vastly increase the potential for abuse of that information."⁶ And finally, in US Department of Justice v. Reporter's Committee, the Court found that a "strong privacy interest inheres in the nondisclosure of compiled computerized information...."⁷ It is precisely the great volume of and easy access to transactional information which raises an increased privacy interest in these records.

V. Extend the spirit of ECPA to cyberspace: Need to update ECPA protections for transactional information in the changing digital world

The guiding principle of ECPA was that new privacy protection should be extended to electronic communications, so that users of new communications technology would have confidence that their communications were free from unwarranted private or government intrusion. With the qualitative shift in communications activity that has occurred over the last decade, it is time to extend greater protection to the transactional information that records people activities online.

A. Gaps left by 1986 law -- Unclear definition of transactional records

The main focus of ECPA was to offer clear privacy protection for the contents of electronic communication despite the fact that the communication is handed

⁵ H.R. Rep. No. 1416, 93d Cong., 2d Sess. 3, 6-9 (1974) Legislative history of the Privacy Act of 1974.

⁶ 429 U.S. 589, 607 (1977) (Brennan, J., concurring)

⁷ 489 U.S. 749, 766 (1989)

over to a third party, namely the electronic communication service provider.⁸ However, little consideration was given at the time to the proper treatment of transactional records. The records are mentioned in the statute, but not given any definition. The committee report from the Senate does offer brief discussion of the nature of these records, but focuses primarily on customer lists and telephone toll records.⁹ The House report recognizes that electronic communications services create records that do not conform to legal categories for older technologies:

The newer technologies such as electronic mail and remote computing services maintain a type of records which do not neatly fit within the legal categories which exist for older technologies.¹⁰

However, nowhere in either committee report is the issue of access to email transactional records discussed for the purposes of establishing the appropriate standard for government access.

B. Extension of protection is consistent with the spirit of ECPA and the expressed intent of the drafters

In the spirit of ECPA, we should recognize that it is again time to extend privacy protection to the personally identifiable transactional information that is, in many cases, indistinguishable from content.¹¹ The drafters did not intend that electronic communication service providers should not disclose "profiles" of users that were related to the contents of the communication.¹² Furthermore, discussions of transactional records was limited at the time to telephone toll records and other customer account billing and demographic information.¹³

⁸ "A letter sent by first class mail is afforded a high level of protection against unauthorized opening by a combination of constitutional provisions, case law.... But there are no comparable Federal statutory standards to protect the privacy and security of communications transmitted by new noncommon carrier communications services or new forms of computer technology. This is so even though American citizens and businesses are using these forms of technology in lieu of, or side-by-side with, first class mail and common carrier telephone services." ECPA Senate report, p5.

⁹ "Subsection (c) provides for access to records or other information pertaining to a subscriber to or customer of an electronic communications or remote computing service, not including the contents of electronic communications. This section permits the provider of the service to divulge, in the normal course of business, such information as customer lists and payments to anyone except a Government agency. It should be noted that the information involved is information about the customer's use of the service not the contents of the customer's communication." ECPA Senate Report, p. 38

¹⁰ House Report, p. 26

¹¹ Curiously, the original language in Title III, before it was amended by ECPA, provided that the "contents" of a communication included the "identity of the parties to such communication or the existence, substance, purport, or meaning of the communication." Thus, in 1968, telephone toll records were accessible under a lower standard precisely because they did not reveal the identity of communicating parties or the existence of the communication. Any transactional information which reveals the identity of the parties, or the content of the communication, should therefore be accessible to law enforcement only with a court order.

¹² ECPA House Report, p.64

¹³ "The type of records involved are billing records and telephone toll records (including record of long distance numbers and message unit information." ECPA House Report, p. 69.

VI. Conclusion

This memo has shown that:

- transactional records now reveal the content of communication,
- these records contain personally identifiable information,
- disclosure of such records implicate fundamental privacy and free association rights,
- current law is unclear as to the definition of such records, and,
- increased protection for transactional records is consistent with the spirit of the 1968 Act and the 1986 Act.

Therefore Congress should amend the stored communications section of ECPA (Sec 2703) to provide a higher level of protection for sensitive transactional records. The amendments would leave intact law enforcement's current authority regarding telephone toll records and basic billing information such as subscriber billing address and service arrangements. These changes to current law are necessary to provide assurances to users of new communication technology that their private activities in the online world are free from unwarranted interference.

For more information, please contact the Electronic Frontier Foundation:

Jerry Berman, Executive Director <jberman@eff.org>
Daniel J. Weitzner, Deputy Policy Director <djwt@eff.org>

Appendix A

Telephone Toll Records and Electronic Mail Logs

The most significant difference between a telephone toll record and an electronic mail log is that electronic mail addresses are unique to individual users. Unlike a telephone number, which corresponds only to a specific location (such as a home or business address), most electronic mail addresses are linked by a secret and unique password¹⁴ to an individual regardless of physical location. Thus, while a record indicating that a certain telephone number was dialed from another telephone number indicates that a transaction occurred, an electronic mail record indicates that a specific and unique individual has communicated with another individual or group of individuals.

Telephone Toll Records

The table below represents actual telephone toll records of a member of EFF's staff, obtained with his consent from Bell Atlantic¹⁵.

```

202 222 2222      JUL 17 94 *IC      LIVE P      7      B      26 1FR
JONAH SEIGER      PB 8146 RT 45      AC 2-00      DEP 5
APT XXX           R1      INCL 300 CT      DDI 123456      LUC
XXXX XXXXXXXX RD NW      R2 8147 NT C      NOB      TAX F-L-S      LCR 12
WASHINGTON DC 20009-2015      CI ELECTRONIC FRONTIER FOUNDATION STAFF 347-
                                     5400

```

```

----AT&T-----
NO      Amount      Place      Number      Date      Time      RATE      Min
1      4.62      SAN FRAN      CA      415 555-5555      JUN 18      1225P      *N      30      J8J1
2      .14      DETROIT      MI      313 555-4545      JUN 18      434P      *N      1      J8J1
3      4.00      OSSINING      NY      914 555-2323      JUN 20      826P      *E      25      J8J1
4      5.25      DETROIT      MI      313 555-4545      JUN 22      900P      *E      30      J8J1

RP      NOTATION      TYPE PN ACT FU BD CMT-TIME 0974

```

These records indicate the date, number dialed, its location, time, and duration of calls made from 202 222-2222, which is billed to Jonah Seiger. These records do

¹⁴ All commercial on line services (AOL, Compuserve, Prodigy, etc), as well as most Internet providers require users to enter a password each time they log onto the service. Passwords are unique to each individual (similar to a PIN number used for cash machines at Banks), and in most cases the practice of using another persons password without permission is considered a breach of contract or user agreement.

¹⁵ The dialed numbers have been changed. The information described above has been certified by Bell Atlantic to be identical to information obtainable by law enforcement officers with proper subpoena authorization. Records indicate long distance toll calls. According to Bell Atlantic, only long distance dialed number records are collected. Law enforcement must use pen register or trap and trace devices to capture local dialed number records.

not indicate that Jonah Seiger himself actually placed the calls, the identity of the recipients, or the nature of the communication (i.e. voice, modem, fax, etc).

Electronic Mail Logs

The table below represents actual electronic mail logs from the Electronic Frontier Foundation's electronic mail server. These logs indicate a message sent by an individual user (in this case, djw@eff.org) to members of an online discussion titled <eff-crypto> (EFF's online forum on issues relating to cryptography and digital privacy in general). Although this example contains addresses unique to EFF, virtually all electronic mail software logs transactions in an identical way. In the course of accounting and processing electronic mail messages, the mail server assigns each message a unique message ID number. By tracking a message ID number, one can easily know who sent a message, and to whom that message was sent. (For ease of reading, line numbers have been added, and message ID numbers are indicated here in **bold face type**).

```
01 7/29 08:15:48 IIA12559: from=<djw@eff.org>, msgid=<199407291215.IIA12559@eff.org>
02 7/29 08:15:49 IIA12559: to="/usr/local/etc/cryptochiver" stat=Sent
03 7/29 08:15:50 IIA12559: to="/usr/local/etc/dmail2list eff-crypto eff-crypto-explorer",
04 7/29 08:15:51 IIA12565: from=owner-eff-crypto, msgid=<199407291215.IIA12559@eff.org>
05 7/29 08:15:51 IIA12565: to=gnu@toad.com (John Gilmore), delay=00:00:01, stat=queued
06 7/29 08:15:51 IIA12565: to=mkapor@kei.com (Mitchell Kapor), delay=00:00:01, stat=queued
07 7/29 08:15:51 IIA12565: to=jberman@eff.org (Jerry Berman), delay=00:00:01, stat=queued
08 7/29 08:15:52 IIA12565: to=jseiger@eff.org (Jonah Seiger), delay=00:00:01, stat=queued
09 7/29 08:15:51 IIA12565: to=djw@eff.org (Danny Weitzner), delay=00:00:01, stat=queued
```

The table above follows a message sent by <djw@eff.org> to the recipients of the <eff-crypto> mailing list. Line 01 indicates that message IIA12559 was sent by <djw@eff.org>. Line 03 indicates that that message was sent to the address <eff-crypto>. Line 04 indicates that message IIA12559 was sent from <eff-crypto> as message IIA12565. Lines 05 through 09 indicate that message IIA12565 was sent to specific individual recipients of the <eff-crypto> list.

Comparison of Telephone Toll Records and Electronic Mail Logs

From these two examples, it is clear that electronic mail logs reveal a great deal more about both the destination and substance of a communication than does a telephone toll record. While the telephone toll record does show that a specific number was dialed at a certain time, it reveals nothing else about the nature of the communication, or the identity of the sender or the recipient. There is nothing inherent in a toll record to indicate that a specific individual communicated with another. In the example above, we only know that 202 222 2222 dialed 313 555-4545 on a certain date and time.

In contrast, because each electronic mail address is linked directly to an individual with a password unique to that address, a record of a communication in this medium indicates the occurrence of a communication between two specific individuals. Moreover, in the example above, the log reveals that an individual communicated with a group of individuals who belong to a subject specific group (in this case <eff-crypto>). Through a simple analysis of message identification numbers, one can very easily track the communications of one person, and know with certainty with whom that person is communicating.

Appendix B

File Transfer and Retrieval Logs

Tracing a File Directly to an Individual

Virtually all online information services, such as America On Line (AOL), Prodigy, Compuserve, and the Internet, contain a wealth of files and information in areas known as "file archives". There are many thousands of archives throughout cyberspace, containing files ranging from political information (e.g.: White House press releases, legislation, policy statements, etc.), shareware (free, public domain software), to images from the Hubble Space Telescope. Users can access file archives through a variety of ways depending on the service they subscribe to.

For purposes of maintenance, accounting and security, most online services keep records of all transactions involving file transfer and retrieval. Through a simple analysis of these records, one can easily trace a file directly to an individual user.

The example to follow will illustrate how such a trace can be accomplished using transactional records from the Internet File Transfer Protocol (ftp), the primary method for transferring and retrieving files over the Internet. FTP provides any Internet user with the ability to retrieve files from any computer on the network. Files available via ftp are stored in 'ftp archives' which can be accessed by a user through the execution of a few relatively simple commands.

Every user on an online network is identified by an electronic identity, usually identical to their electronic mail (email) addresses. Individuals control access to their email addresses through a secret personal password. Because email addresses are tied to individual users, and because ftp logs indicate that a specific file has been retrieved, a simple analysis of ftp logs can easily reveal that an individual has retrieved a specific file.

FTP Transaction logs

This example will trace an individual user's retrieval of a file from the online archives of the Electronic Frontier Foundation (EFF). The file, named 'digitel.faq', contains answers to frequently asked questions about the Digital Telephony legislation. The records below are actual records from EFF's ftp archive (named <ftp.eff.org>) and main computer (<eff.org>)

All computers connected to the Internet have names. In this example, it is important to note that <ftp.eff.org> and <eff.org> are two distinct computers. The computer <ftp.eff.org> keeps separate records from the computer <eff.org>. Furthermore, each authorized user has a unique electronic identity, usually same as that individual's electronic mail address (e.g.: brown@eff.org is the user Dan Brown [EFF's system administrator]). A simple correlation of the timestamps on the transactions between the two computers will reveal that Dan Brown retrieved the file 'digitel.faq'.

I. Dan Brown Logs Onto <eff.org>

By examining the logs of the computer `eff.org`, we can determine when a specific individual logged onto and off of the network. This record is displayed below:

```
* User Terminal Remote machine Timestamps
05 brown ttyp0 elec.eff.org Fri Jul 29 12:59:04 - 13:03:14
```

Because the user 'brown' is linked to Dan Brown through a unique personal password, this record indicates that Dan Brown was logged onto <eff.org> on Friday July 29 between 12:59 and 13:03.

II. Dan Brown Executes a File Transfer (ftp)

By examining the logs which record the programs run by users on <eff.org>, and noting the times at which those programs were run, we can determine when Dan Brown executed a file retrieval program (ftp). This record is displayed below (printed on July 29 at 13:15):

```
* program user name terminal start time end time
08 ftp brown ttyp0 13:00:21 13:01:20
```

Note that the start and end times correspond to the period of time Dan was logged onto <eff.org>. This record clearly shows that Dan Brown ran the file retrieval program (ftp) between 13:00:21 and 13:01:20.

III. Logs from the File Archive Show a File Transfer

We now turn our analysis to the records of the computer containing EFF's online file archives (the computer named <ftp.eff.org>). Again, a simple check of timestamps reveals that a user from <eff.org> made a connection using the file transfer program (ftp). These records are displayed below:

```
* Timestamp Hostname Process ID Message
04 Jul 29 13:00:21 ftp.eff.org in.ftpd[5458]: connect from brown@eff.org
12 Jul 29 13:01:20 ftp.eff.org ftpd[5458]: FTP session closed
```

Note the direct correlation between the times indicated above and the times indicated on the previous two logs. This log shows that the file transfer program run by Dan Brown was executed on the computer <ftp.eff.org>, indicating that Dan Brown retrieved a file from EFF's online file archive.

IV. Logs from the File Archive Name the File Transferred to Dan Brown

One final check of the logs from EFF's online archive show which file Dan transferred to his own computer. We already know that Dan was logged onto the network between 12:59:03 and 13:03:14. We also know that he ran the file transfer program between 13:00:21 and 13:01:20. This has been confirmed by logs from two separate computers. By examining one additional log on the computer containing EFF's online file archive (<ftp.eff.org>), we can see which particular file Dan retrieved. This log is displayed below:

```

Fri Jul 29 13:01:18 1994 1
                        eff.org
                        67773
/pub/EFF/Policy/Digital_Telephony/digital.faq

```

This log shows that the file 'digital.faq' was retrieved at 13:01:18 by a user logged onto the computer <eff.org>. Note that the exact time of the file retrieval corresponds to the time that Dan Brown was running the file retrieval program (as indicated on the logs described previously).

We have seen that Dan Brown was running the file retrieval program between 13:00:21 and 13:01:20. This is confirmed on the logs from both the computer Dan was logged onto (<eff.org>) as well as the computer containing the online file archive (<ftp.eff.org>). Because the logs also show that the only user running the file transfer program at that time was Dan Brown, we have now confirmed that Dan Brown retrieved the file 'digital.faq'.

FTP Logs Reveal the Actions of an Individual User and the Contents of those Transactions

Detailed transactional information from online information services enables anyone with access to these records to reconstruct a detailed picture of a user's actions. In this case, the logs show which document the user accessed. Because all users on the Internet and other online services are linked to their electronic identities by a unique password, transactional records which reveal the electronic identity of a user correspond directly with that individual. The electronic identity <brown@eff.org> is always Dan Brown. In the case of this example, transactional records reveal that Dan retrieved the file 'digital.faq' from the online archives of the Electronic Frontier Foundation.

Transactions similar to the one illustrated here occur millions of times each day on computer networks throughout the United States. Furthermore, because computer logs record each and every transaction, it is not difficult to track the actions of any individual using an online service simply by examining such logs.

This type of detailed transactional information is not unique to Internet ftp sessions. It is captured in similar forms on computers throughout the online service world. Every time a user logs on to an online service, sends electronic mail, retrieves a file, or joins a discussion group, detailed information is collected in the normal course of completing these transactions. And, since virtually all users of online services are personally linked to their electronic identities by a unique password, all of these transactional records point directly to the actions of individual people.

Mr. MARKEY. Our next witness, Mr. Tom Wheeler, is the president of the Cellular Telecommunications Industry Association; and in his position, as well as in a previous position at the cable industry, he has been testifying before this subcommittee for some 15 years now and is, without question, one of the most respected experts in communications in the country.

We welcome you back before us, Tom. Whenever you are ready, please begin.

STATEMENT OF THOMAS WHEELER

Mr. WHEELER. Thank you very much, Mr. Chairman.

As you indicated, I am here on behalf of probably the greatest revolution in telecommunications, at least since the Second World War. And we heard the discussion on the first panel, talking about how we had to keep up with the revolution in technology; and many of the examples cited were the wireless telecommunications industry.

We concur with the discussion that we heard you all talking about with the previous panel, that really what we are talking about here is a piece of legislation which is substantively sound but fiscally flawed. When you look at the legislation, it is very specific in terms of the requirements it places on industry. It is very precise on the penalties that it establishes for industry, and it is very imprecise on the requirements to be upheld by the government, such as what are the capacity expectations, both short term and long term?

What are the means for determining what those capacity expectations should be? What are the cost estimates and how are you going to pay for it?

Mr. Boucher and Mr. Wyden raised the issue of public accountability. We agree that is the issue that needs to be dealt with, because really what we are talking about here is an unfunded mandate. We are talking about certainty for the FBI and law enforcement agencies in terms of the requirements that they will impose on new technologies, and uncertainty for those on whom it would be imposed, both in the short term and the long term.

But let me be very clear: we support what this legislation intends to accomplish. We want to help catch crooks. We have been helpful in catching crooks. In 1993, the cellular industry had less than 5 percent penetration, yet 25 percent of all the wiretaps conducted in the country, by the FBI's own count, were conducted on cellular systems. That is cooperation. That is working to make sure that the new technology is available for lawful surveillance.

This bill does a good job in two areas. It is a vast improvement over the earlier draft in that it reflects how wireless telecommunications works, and we should give the appropriate kudos and credit to both the FBI and the Judiciary Committees for their efforts in this regard.

The second major thing that the bill does hasn't been discussed today, however, and that is that it also outlaws the technologies which are created for the purpose of defeating identifying wireless users. We have all heard the stories about somebody who opens their cellular bill and finds out that it is some great size because

somebody has cloned the phone illegally and has been charging calls to their digital identification number.

Not only is this harmful to consumers, but it also defeats law enforcement, because if you have the ability out there to clone a number and to pretend that you are somebody else, if you will, then who do you tap? And more importantly, even, when you get to court, how do you prove that it was the person with whom the phone was registered or one of the multiple number of people who may have cloned that person's phone? And, incredibly, our laws today do not make it a crime to fraudulently clone and impersonate somebody else's identification number in a wireless environment. This bill does that and, therefore, is an important step forward in law enforcement, as well as in consumer protection.

I reiterate to you that this surveillance capacity, capability discussed in this bill should become law, but before doing so, the procedural shortcomings in the bill must be fixed. The Congress must link compliance requirements to the reimbursement promised by the government, and that is not what the bill does.

The bill says, trust us. The FBI demands specificity in what is imposed on the industry, but there is no right on the part of the industry in this bill, as presently drafted, to expect the same kind of specificity from the government. We don't know how the specificity required in the bill is going to be implemented.

There has been a lot of talk today about how in Findlay, Ohio or Humble, Texas, or in Blacksburg, Virginia, the demands are different than in Boston. Absolutely. As the chairman pointed out, 50 percent of all the cellular wiretaps were in two States, 80 percent were in six States. That suggests the need for graduated requirements.

But we also heard the Director say this morning that maybe there shouldn't be graduated requirements because of the migration of the bad guys. So what are we to expect in terms of what this bill will require? And because we don't know what the expectations are, we don't know what the cost is. The GAO says it could cost several billion to implement this. That is why we call it an unfunded mandate. It, in essence, says to the wireless industry, obey the law, spend the money and then we will see if we can reimburse you.

The Director talked about a "safe haven." Well, the court could always fail to impose a penalty on you because the funds have run out. That is backwards. We want to salute the flag, say, yes, sir, we will implement the law, and not have to quibble down the road in some court. Let's do what needs to be done to catch the bad guys.

It seems to me that there is—yes, sir, Mr. Chairman. It just seems to me there is a metaphor that when the FBI goes to Detroit and says, we need a vehicle, a special vehicle for law enforcement purposes, they don't say, build it and then we will see if we can pay for it. They say build it, here are the specs, here is the purchase order. That is the kind of certainty that we are asking for in this.

We are asking this committee, yes, to update the wiretap laws, but also to link those requirements to the funding thereof.

Thank you.

Mr. MARKEY. Thank you, Mr. Wheeler, very much.
 [The prepared statement of Thomas E. Wheeler follows:]

STATEMENT OF THOMAS E. WHEELER, PRESIDENT AND CEO, CELLULAR
 TELECOMMUNICATIONS INDUSTRY ASSOCIATION

The commercial mobile wireless telecommunications industry appreciates the opportunity to appear before you today to discuss our industry's involvement in meeting law enforcement's surveillance requirements.

The Cellular Telecommunications Industry Association ("CTIA") was organized in 1984. Over the past 10 years its membership has grown to encompass all aspects of two-way wireless telecommunications (known as "commercial mobile services"), including licensed cellular, personal communications services, enhanced specialized mobile radio, and mobile satellite services. The association also counts as members the wireless service providers in Canada and Mexico, equipment and infrastructure manufacturers, and others with a general interest in the wireless industry.

The wireless decade began with pioneers from both large and small companies taking risks to create a nationwide cellular network. Since its inception in 1983, private entrepreneurs have invested more than \$16.1 billion in wireless infrastructure. Today, more than 300 cellular carriers provide service to over 19 million Americans in every one of the Nation's 734 metropolitan and rural service areas. As of June 1994, more than 45,000 people are directly employed by the cellular industry; another 120,000 are employed in related industries.¹ In less than 10 years of operation, the cellular industry has created over 165,000 jobs for Americans.

When a subscriber makes a call on a wireless phone, as shown in Exhibit I, radio waves are transmitted to the nearest tower. By constructing the network using small low power cells, wireless technology reuses the same radio frequencies and, thus, can handle a large number of simultaneous users. Instead of having a radio channel, like Citizen's Band radio, that reaches across a market and must be shared by everyone, low power, limited reach wireless cells permit the channel to be used again and again. The ability to travel between cells is achieved by a sophisticated signal strength monitoring and computer control system which senses when a caller is leaving a cell and hands that call off to an adjacent cell.

Once the communications signal is received at the cell tower, the "wireless" component of the transmission is over and more traditional technologies take over. From the cell tower the system transfers the call to the mobile telephone switching office ("MTSO"). The MTSO is the wireless system's equivalent of the landline local exchange central office switch. At the MTSO, the subscriber's connection is monitored by wireless messages to and from the subscriber's unit on a control channel separate from the voice channel. The MTSO reads the information contained in the control channel and, depending upon the information received, routes the subscriber's call to the public switched landline network, a long distance carrier, or to another mobile unit in the service area. Exhibit I, *see supra*, illustrates how a wireless call is transmitted.

If a subscriber travels beyond the home carrier's geographic area and makes calls on his/her wireless phone, the local carrier in that market will provide the service. This is known as roaming. Wireless carriers allow their customers to use each other's service by executing carrier-to-carrier roamer agreements. These agreements mainly specify which services each carrier will offer roamers, and how the carriers will exchange information to permit timely and concise billing for services rendered on each carrier's system.

The billing information exchanged between carriers passes through a series of industry standardized edits, ensuring that billing information which appears on a subscriber's bill is consistently timely, error-free and easy to understand. Each carrier submits its own figures for revenue owed and due through a central bank, which in turn performs a net financial settlement process. CIBERNET Corporation, a subsidiary of CTIA, administers this program of net settlements for the industry.

Roaming connections are more challenging than calls made within the home system. But today, thanks to roaming agreements and the IS-41 signaling protocol, subscribers can use their telephones throughout the Nation. The IS-41 technology is particularly important in a law enforcement context because it permits systems to send data regarding a specific call to each other.

Exhibit II illustrates how, when a wireless phone is turned on and registered in a roaming market, an IS-41 message is automatically sent to the home system. This message asks if it is OK to provide service to the phone and what special services

¹ CTIA Semi-Annual Data Survey, June 1994.

or features the subscriber uses. The IS-41 message then permits the home MTSO to route calls to the subscriber in the roaming market.

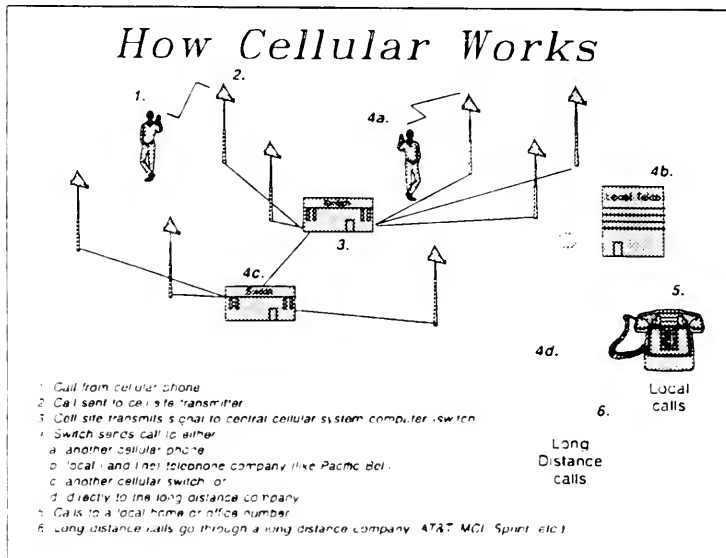


Exhibit I

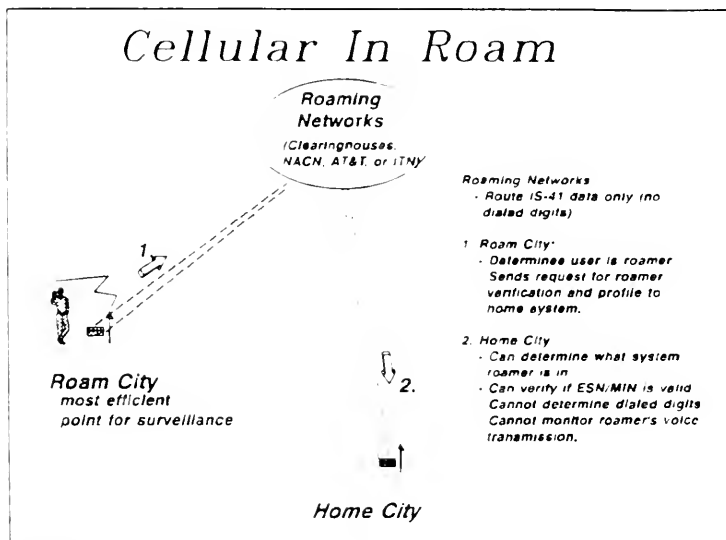


Exhibit II

The wireless telecommunications industry is relatively young, and one which has experienced explosive growth after its "start from scratch." No less an expert than AT&T, the developer of cellular technology, forecast that by the year 2000 there would be only 900,000 cellular subscribers. In its early years, the challenge was to survive and make the technology work. The wireless industry's pervasive impact on society is a relatively new development which has brought with it uses for ill, as well as innumerable uses for good.

With such an impact on society goes responsibility, in this case the responsibility to look beyond survival and technology to the role of the industry in the community. This includes the responsibility to support law enforcement's ability to lawfully intercept wireless communications. The wireless industry has assumed its responsibility to law enforcement. Cellular carriers were utilized in the execution of nearly 25 percent of the FBI's estimated 976 electronic surveillance court orders executed at the Federal and State levels throughout the Nation in 1993.²

Twenty-five percent of all wiretaps is illustrative of how the wireless industry has been responsive in the manner in which it has supported law enforcement. Unfortunately, for security reasons law enforcement typically asks carriers not to discuss their success in call interdiction. Thus, it is difficult to portray the many successful instances of joint cellular-law enforcement efforts which exist. Occasionally, however, one story does find its way into the press and, then, can be discussed. One such story is how a cellular company's prompt action saved a life and resulted in a special citation from the FBI. Working with law enforcement, Cellular One in New York, used wireless intercept technology to assist the FBI in apprehending the kidnappers of Harvey Weinstein, the New York clothier who was kidnapped for ransom and buried alive. The cellular carrier was able to determine where the victim was located after his captors forced him at knife point to make a short cellular telephone call to his family to demand ransom money. Cellular One was not only able to record the call detail, but was also able to determine from where the call was placed. During the 2-week investigation, critical investigatory information was obtained by the FBI through the cellular network. This information led to the rescue of the kidnap victim, the arrest of the kidnappers, and the recovery of the ransom money. Exhibit III is a reproduction of a news article reporting on this story, including an award of recognition presented by the FBI.

CELLULAR PLAYS KEY ROLE IN KIDNAPPING CASE

[by Robin Susan Traum]

Federal and local law enforcement agencies used cellular technology and the expertise of Cellular One employee Joe Radicella to solve a recent kidnapping case in New York.

Harvey Weinstein, president of a New York tuxedo company, was abducted at knife point in early August while on his way to pick up his daughter at the airport. It was when the kidnappers forced Weinstein to make a cellular phone call to his family demanding ransom that the FBI contacted Cellular One for assistance.

Radicella, a Senior Switch Technician in New York New Jersey, sorted through stacks of records and raw data looking for information on the short cellular call Weinstein made to his family. After hours of research, Radicella determined the call was placed from a counterfeit cellular telephone. Over the next several days, Radicella provided the FBI with other information critical to their investigation.

With this information, authorities were able to locate Weinstein after he had been held captive for nearly 2 weeks in a deep pit alongside one of New York City's busiest highways. Shortly thereafter, the police arrested his kidnappers and recovered the ransom money.

At a ceremony at Cellular One's Paramus, NJ offices, two special agents presented Radicella with a special letter of commendation from the FBI and U.S. Department of Justice for his invaluable assistance in helping solve the kidnapping that drew national media attention. In the letter, Radicella's efforts were described as yielding very significant investigative information and instrumental in the successful resolution of the Harvey Weinstein Kidnapping case. It recognized Radicella for his "exemplary work, positive attitude and professionalism which reflect most favorably upon Cellular One."

In addition to their more routine daily uses of cellular telephones, law enforcement agencies in the New York/New Jersey market typically make 25 to 30 requests each year for specialized technical assistance in criminal investigations.

It is not only right that wireless providers should assist law enforcement in this way, it is the law. In a 1970 amendment to Title III of the Omnibus Crime Control and Safe Streets Act of 1968, Congress enacted a provision specifying that a "communication common carrier shall furnish the government applicant for court-ordered electronic surveillance with all information, facilities, and technical assistance necessary to accomplish the interception."³ While the current law is clear, unambig-

² Source: Administrative Office of the United States Court, Wiretap Report, January 1-December 21, 1993. See attachment A.

³ 18 U.S.C. section 2518(4).

uous and working, the wireless industry fully understands the concerns expressed by the FBI of the need to keep law enforcement agency capabilities current with new technology in the rapidly evolving telecommunications industry.

The telecommunications industry, including the wireless industry, has continued to work closely with the law enforcement community to resolve technical and electronic surveillance problems. As further evidence of this cooperation, in March 1993, the Board of Directors for the Alliance for Telecommunications Industry Solutions, (ATIS), formerly the Exchange Carrier Standards Association, (ECSA), approved a request from the industry and law enforcement agencies to sponsor a committee to identify those technical and associated operational issues related to lawfully authorized electronic surveillance and to develop resolutions to such issues for voluntary implementation by the industry. That committee is the Electronic Communications Service Provider (ECSP) Committee.

ATIS is a not-for-profit corporation, established for the purpose of promoting timely resolutions of national and international issues involving telecommunications standards and the development of operational guidelines. ATIS initiates and maintains open industry forums to address technical and operating issues affecting the Nation's telecommunications facilities and services, and the development of innovative technologies. ATIS serves as an information resource to its members, its forum participants and other interested parties. It promotes industry progress and harmony with minimal regulatory or legislative intervention.

This government/industry group had been meeting for more than a year prior to its request for ATIS sponsorship. In order to continue the group's momentum, there was a period of transition to full ATIS sponsorship. The first meeting of the ECSP Committee under ATIS auspices occurred on September 1, 1993. The committee has adopted a set of Operating Principles, and selected committee co-chairpersons; one from the industry and the other representing law enforcement.

Membership in the ECSP Committee is open to all providers of electronic communications services, as defined in section 2510, Title 18 of the U.S. Code, U.S. law enforcement agencies that are empowered to perform lawfully authorized intercepts of communications, telecommunications equipment manufacturers, and others, such as trade associations, subject to ECSP Committee approval. Due to the sensitive nature of the information that is discussed at ECSP Committee meetings, attendance and access to ECSP Committee information is limited to ECSP Committee members and invited guests who have signed a non-disclosure agreement.

Industry membership presently includes all of the major local exchange carriers, (LEC's), interexchange carriers (IC's), major equipment manufacturers such as AT&T, Northern Telecom and Siemens Stromberg Carlson, cellular service providers, and industry trade associations such as United States Telephone Association (USTA), and the Cellular Telecommunications Industry Association (CTIA). Law enforcement membership comes from many city, county, State and Federal law enforcement organizations.

The committee operates through Action Teams, which study specifically identified and designated issues. These issues focus on sophisticated communications technology, identified by the committee, which impact on the ability of Federal, State and local law enforcement agencies to conduct court-approved electronic surveillance. The Action Teams identify potential solutions, which are made available to the participants for voluntary implementation in their networks.

The efficacy of this kind of government/industry cooperation and coordination should not be discounted in determining how to legislatively address electronic surveillance issues in a timely and cost-efficient manner.

In order to fully understand the issues involved in this debate, it is necessary to understand how a wireless system works to facilitate a lawful wiretap. As described previously, when a subscriber places a call from a mobile unit, the call comes to the MTSO. The MTSO, or switch, is a sophisticated computer that processes the call and routes it where it needs to go (see section II, *supra*). Each switch contains several "ports," as do most computers, which allow access to the programs and processes that take place internally. Because they are essential to conducting maintenance, all switches have ports. It is at this point, using an available port, that the call content and call detail information can be intercepted.

While switches, usually in the major markets, have sufficient port capacity, a particular MTSO may need additional port capacity because of heavy wiretap demands in that market. Such additional port capacity can be added, within the limits of the physical surroundings of the switch. Typically, such capacity comes in banks of 24 ports which costs around \$200,000 per bank with associated software.

When a wireless user roams, the tap occurs in the same way at the MTSO in the distant market. The IS-41 network, discussed above in section II, alerts law enforcement that the suspect has moved and identifies the new location. With this informa-

tion, a lawful warrant can be obtained from the proper court and the tap can be put on the MTSO at the new site. It should be noted that this capability is switch-dependent and some in-service wireless switches will need to be upgraded. The cost of such upgrades will vary depending on the type and quality of switch in service, but can be expensive.

There are two types of information which law enforcement seeks through wiretaps. One is the information regarding the call, that is, the number dialed and other "call setup" information. The other information is the content of the call itself (the conversation or the data transmitted during the call).

Call setup information is the MTSO's resident internal data that is used to establish a link to the cellular subscriber. This information contains: (1) call destination (dialed digits); (2) identity of the location of the incoming call; (3) date, time, and duration of the call; and (4) first and/or last cell site used to deliver the call.

All cellular switches provide call setup information. The only issue is how quickly it is available. As a call is completed, the call detail information is stored in the switch's billing records data element and every 24 hours those records are transferred into a data base, at which time the call detail information can be withdrawn. Thus, any cellular system today can provide call detail in an average time of 12 hours. Recognizing law enforcement's desire for immediate call detail information, software has been developed which can pull the call detail immediately upon completion of the call. This capability has been developed without legislation and is now available on switches made by three of the four major switch manufacturers. The average cost for such capability is \$50,000.

Dialed digits can be obtained pursuant to what is called a "pen register" warrant. However, pen register warrant authority does not grant law enforcement access to call content. Pursuant to a Title III warrant, law enforcement may obtain call content information on a real-time basis. In order to obtain call content information, law enforcement must simply access a port on the MTSO that processes the call.

The House and Senate Judiciary Committees and their professional staff are to be congratulated for substantial revisions that have been made to the original draft proposal put forth by the FBI entitled "The Digital Telephony and Communications Privacy Act of 1994." On the whole, it is a much improved statement of the needs of law enforcement and of the obligations imposed upon the telecommunications industry to meet those needs. We would call your attention to several specific provisions of the legislation:

A. Cellular Fraud—Importantly, in addressing law enforcement's electronic surveillance needs another criminal activity has been addressed in the revised legislation as well. We've all heard the stories of someone receiving a cellular bill for thousands of dollars for calls they did not place. Criminals are utilizing techniques such as "cloning" and "tumbling" electronic serial numbers ("ESN's") to obtain service fraudulently. Cellular companies are presently losing \$1 million a day to fraudulent tampering and alteration of the mobile telephone unit. The proliferation of the fraudulent use of wireless telephones through such techniques is not just a business dilemma, however. If lawbreakers can make one wireless phone impersonate another with impunity and without fear of punishment, then lawful wiretaps can be compromised since neither a wireless carrier's switch nor law enforcement will know which is the "real" number and user right away.

Today, fraudulent alteration of a wireless phone can be accomplished relatively easily. Each phone is originally programmed with a unique electronic serial number (ESN) at the time of manufacture. When a customer purchases the phone and subscribes to a particular carrier's service, a separate mobile identification number ("MIN") is programmed into the phone. This ESN/MIN combination becomes the wireless system's means of verifying the identity of the subscriber (it is this information, for instance, which is hauled over the IS-41 network to allow tracing of a mobile phone to a foreign market). The ESN/MIN is transmitted continuously to a wireless carrier's switch while the subscriber's phone is in the "on" position. The switch verifies that the ESN/MIN combination is a legitimate account and then processes the call.

Utilizing scanner equipment and off-the-shelf software and hardware, a person desiring a cloned phone can capture the subscriber's ESN/MIN off the air and reprogram another phone with that same ESN/MIN combination. Often, the first time there is an awareness that the ESN/MIN has been cloned is when a subscriber reports to his carrier that a bill has been received with charges for calls to points around the country or world that the subscriber did not make. The carrier then must program the switch to discontinue processing calls from that ESN/MIN combination and the subscriber is given a new combination.

There are currently over 19 million subscribers using analog wireless phones and it will be many, many years, if ever, before all analog phones are phased out of serv-

ice and all subscribers are converted to digital. While the introduction of digital technology may slow the pace of cloning temporarily, it can be expected that creative criminal elements and "phone hackers" will soon be able to alter these devices as well.

Altering or reprogramming a wireless phone's ESN or MIN can seriously impact the constitutional and statutory limitations of wiretap procedures as well. A suspect who is using a cloned phone is actually using a wireless communications system's electronic identification of another person without their consent. It is possible then that government will inadvertently intercept one person's private conversations when it thinks it is intercepting another.

In addition to such privacy concerns, the evidentiary ramifications are equally alarming. Because of the existence of cloning, law enforcement cannot guarantee that the content and call detail information it intercepts originates from the suspect who is the target of the wiretap. Thus, it can result in the government being unable to establish the requisite link between the tapped suspect and the intercepted call content/call detail needed to incriminate the suspect.

Even when it becomes apparent that a suspect is using a cloned phone and counter-measures are taken, such as giving the legitimate subscriber a new phone with a different ESN/MIN, there is nothing to prevent the target suspect from merely reprogramming his phone with yet another stolen ESN/MIN of another legitimate subscriber. In fact, today's wireless pirates have the ability to reprogram a phone every time a call is made.

The hardware and software necessary for such alterations are readily available and by themselves are not illegal to possess. The use of these unauthorized counterfeit phones is not clearly a crime either. Section 1029 of Title 18, entitled "Fraud and related activity in connection with access devices," enacted primarily to address credit card fraud, has been the only statutory provision available to the Secret Service and U.S. Attorneys to prosecute these acts. Some Federal district courts, and recently the 10th Circuit Court of Appeals,⁴ have determined that this statute does not cover the possession of cloning equipment or the use of cloned phones even when it is clear from the facts that such possession and use are for fraudulent purposes.

This dilemma can only be remedied by Congressional initiative to clearly make such acts illegal, and then by a concerted effort from law enforcement to work with industry to curtail such activity and the proliferation of the paraphernalia utilized in association with such acts. The wireless industry is pleased to see that this revised legislation contains such an initiative.

B. Capacity Determinations—The manner in which law enforcement determines its wiretap capacity must be done in a very cost-effective manner to ensure that Federal funds are not being unwisely or unnecessarily expended. An area where the legislation, as introduced, should be strengthened is the linkage between wiretap capacity and cost.

The amount of the bill presented to taxpayers will be determined by the size of the wiretap capacity wish list developed by law enforcement. Human nature what it is, one party will want it to be as large as possible, while the other party will seek just the opposite. However, as presently drafted, there is no mediation process to resolve these conflicts, save for a unilateral determination by the Attorney General.

CTIA urges Congress to include in the capacity determination, a notice and comment rulemaking proceeding, just as the legislation presently allows for capability determinations, which affords all parties an opportunity to build a record.

C. Roaming—The introduced legislation addresses the concerns that the wireless industry expressed over the cost and complexity to add capability to retrieve content in a roaming environment. Wireless technology, fortunately, has the capability to advise law enforcement when a target has traveled outside of the home market, and to identify this roaming market in which the target may be using his or her wireless phone. This then, enables a tap to be put on the switch in the distant market.

One of the great improvements made in the legislation is how this capability can be used effectively and at a lower cost than previously proposed alternatives.

D. Cost Reimbursements—The introduced legislation provides that the government reimburse industry service providers for the reasonable costs incurred in establishing the capabilities deemed necessary by law to ensure the ability to continue

⁴The 10th Circuit Court of Appeals recently ruled that section 1029 does not apply to cellular "tumbling" fraud. *United States v. Brady*, No. 93-4085, slip op. at 13-14 (Dec. 21, 1993) ("Although Congress, without question, has the power to criminalize the use of or trafficking in cellular telephones altered to allow free riding on the cellular telephone system, even when such telephones do not access valid identifiable accounts, Congress did not do so when it enacted section 1029").

to conduct lawful electronic surveillance, as well as to reimburse costs incurred to expand capacity to meet the projected demands of law enforcement. It remains, however, an open question as to what will ultimately be the full extent of those costs. Until each carrier examines its system status in light of these legislated capability requirements, and until the Attorney General has quantified the capacity requirements of law enforcement agencies at the State and Federal level, and until price quotes are obtained from manufacturers and suppliers on the necessary changes and additions to these systems, an accurate projection of these costs cannot be known.

CTIA urges the Congress to delay implementation or compliance dates until it has determined these costs elements. Pending implementation, Congress should require both industry and law enforcement to report to it, within 1 year post-passage of this legislation, with: (1) an accurate estimate of law enforcement's capacity needs; and, (2) an accurate assessment of the costs to be encountered by industry to produce and install the capacity and capability requirements. After accurate determinations have been made, Congress can determine the terms, conditions, and timeframes within which such costs should be appropriated and allocated. Without it Congress will grant authority to either sign a blank check for unlimited duration, or impose upon telecommunications subscribers of the various segments of the telecommunications industries affected, increased costs and rates of unknown proportion.

For instance, there are just over 1,100 cellular switches in operation covering 1,550 systems nationwide. However, a review of the wiretap data reveals that of the 225 wiretap executed on cellular systems, 50 percent were performed in only two States. Eighty percent of the total were executed in six States (see Attachment A). While the data does not reveal the cities in each State where the taps occurred, it is likely that only one major city in each State was the principal location.

This kind of information coupled with accurate cost data, can enable Congress to make an informed decision as to whether or not it is a wise use of taxpayer dollars to require outlays for many wireless systems in the Nation to meet the capability requirements, or whether it would be better to establish a method to prioritize necessary system upgrades in relation to wiretap demands over a longer period of time. This would avoid imposing unreasonable demands upon the Federal treasury, and avoid the potential imposition of lengthy delays in the reimbursement of such costs to the telecommunications carriers, where unreimbursed outlays can have a substantial impact on operations, particularly for the smaller and newer carriers.

The principle issue still remaining is how and how much the government plans to pay for the upgrades to carrier systems and whether the obligations to provide upgrades will continue in the absence of government funding. Post-introduction of H.R. 4922/S. 2375, industry and committee representatives continue to meet in an attempt to resolve this issue. The affected telecommunications industry remains firm in its opposition to obligations continuing without comparable law enforcement obligations to pay for system changes or upgrades to meet law enforcement's surveillance needs.

The testimony presented today illustrates that the wireless telecommunications industry has a history of supporting the lawful needs of the FBI and other law enforcement agencies around the country as regards surveillance requirements. It is the industry's intention to continue to work closely with law enforcement to maintain compliance.

To the extent that the Congress deems this additional legislation necessary to fully ensure future capacity and capability of both industry and law enforcement, a careful and reasoned approach to the many issues and the costs attendant thereto is vital, with meaningful input from the affected industry and public interests that have appeared before Congress.

Finally, there is a major criminal activity which is addressed in the introduced legislation by the Congress—the fraudulent cloning of wireless technology that impedes law enforcement, intrudes on consumer privacy and defrauds wireless service providers. We strongly endorse this measure and urge its adoption in full.

Thank you for this opportunity to appear today. I will be happy to respond to any questions that you may have.

CELLULAR WIRETAPS

[Calendar Year 1993]

Location	Federal	State	Total
New York	16	68	84
Florida	18	11	29
Texas	18	3	21
New Jersey	4	12	16

CELLULAR WIRETAPS—Continued
[Calendar Year 1993]

Location	Federal	State	Total
California	11	2	13
Michigan	13	0	13
Pennsylvania	2	6	8
Ohio	4	0	4
Illinois	3	0	3
Kentucky	3	0	3
Louisiana	3	0	3
Missouri	3	0	3
Nevada	3	0	3
Oregon	1	2	3
Arizona	2	0	2
Colorado	2	0	2
Connecticut	2	0	2
WDC	2	0	2
Maryland	0	2	2
Massachusetts	0	2	2
Minnesota	2	0	2
Nebraska	2	0	2
Arkansas	1	0	1
Indiana	1	0	1
Tennessee	1	0	1
Total	117	108	225

Total Wiretaps (all types) for 1993 = 976. Cellular wiretaps for 1993 = 225

Less than one-fourth of all wiretaps are cellular

Source: Administrative office of the United States Court Wiretap Report. For the period January 1, 1993 to December 21, 1993.

Mr. MARKEY. And our final witness is Mr. Daniel Bart, who is the vice president for Technical and Regulatory Affairs of the Telecommunications Industry Association. He is a first-time witness before the subcommittee here today.

We welcome you, sir. Please begin.

STATEMENT OF DANIEL L. BART

Mr. BART. Thank you, Mr. Chairman, members of the subcommittee.

The Telecommunications Industry Association, or TIA, represents more than 550 U.S. manufacturers and suppliers of telecommunications equipment and is pleased to have this opportunity to highlight our testimony and comment on the manufacturing provisions of H.R. 4922 and on the financial implications of the digital telephony issue.

This bill represents a significant improvement over FBI digital telephony proposals circulated in 1992 and 1994. Accordingly, while the TIA strongly prefers continued efforts under current law to foster cooperation between law enforcement and manufacturers, such as in the form of an electronic communication service provider committee, the TIA believes that further refinement of H.R. 4922 could yield legislation which will both accommodate the legitimate needs of law enforcement and safeguard the interests of telecommunications equipment manufacturers.

Refinements are necessary, and they include some in the manufacturing provisions of the bill. These include things such as, who defines what is a reasonable charge? Who pays for the modifications? Do we need penalties for manufacturers' failure to comply? And what triggers the FCC's authority to set the standards?

And an issue we have talked a lot about this morning, what are the costs? Who defines what constitutes a reasonable charge for equipment modifications required under subsection 2605(b)?

The price that manufacturers of transmission and switching equipment charge for their products has historically been determined by market forces. This reliance on market forces has created a robustly competitive market for the manufacture and sale of telecommunications equipment and has encouraged technological innovation.

The subcommittee should seek to ensure that the present reliance on market forces is not disturbed, and thus should take care to explain that it is not the subcommittee's intent for the FCC, or any other agency of the Federal Government, to regulate the price of telecommunications transmission and switching equipment. The TIA regards regulation as unnecessary in what is a truly competitive marketplace and asks the subcommittee to clarify that determinations regarding what constitutes a "reasonable charge" for modifications should be made by manufacturers, in consultation with their customers, in accordance with normal business practices.

Additionally, TIA urges the subcommittee to clarify 2605(b) to indicate that when a manufacturer undertakes such modifications as are necessary to permit its customer, the carrier, to comply with the bill, the manufacturer is to be paid by the carrier in accordance with normal and accepted business practices. A manufacturer of equipment has only a single source, its customer, from which to seek compensation for the cost.

The second matter of concern to TIA is the possibility that manufacturers will face civil penalties if they fail to comply with the requirements of the bill. Under normal business practices, telecommunications carriers set forth the technical requirements when they contract for equipment. After such communication, the manufacturer is compelled by the contract to provide the modifications that are required. TIA is less comfortable, however, with the provision of 2607(f) that would subject the manufacturer which fails to provide necessary modifications to a civil penalty of up to \$10,000 per day for each day such manufacturer is not in compliance with the requirements of the bill.

There is no need to apply significant penalties to manufacturers since there is an existing marketplace mechanism to ensure manufacturer compliance. TIA believes market considerations will adequately ensure manufacturer compliance and accordingly, TIA considers imposition of civil penalties on manufacturers totally unnecessary and counter to the cooperative spirit embodied in the bill.

The third issue is when the FCC may involve itself in the standards-setting process. Under subsection 2606(b), the Commission is authorized to set standards if private sector standards-setting bodies fail to do so or if a government agency or other person believes that such standards are deficient. It requires neither a specified time period within which private sector bodies are allowed to perform these activities prior to Commission involvement, nor any demonstrable showing that a standard is in fact deficient.

TIA urges the subcommittee to clarify 2606(b) to require private sector bodies to have a reasonable opportunity to act prior to FCC involvement and to strengthen the criteria which an agency or indi-

vidual challenging a standard must meet in order to show that the standard in question is deficient and to compel Commission involvement.

The final issue we heard this morning is cost. The matter of cost remains largely unsettled in TIA's view. To a great extent, capability and capacity specifications will determine the costs, and until the law enforcement community makes clear its expectations for such requirements, all cost estimates are highly speculative. However, it is possible to identify ranges where costs are likely to fall, and on the basis of that information, we conclude the \$500 million authorized by the bill will be insufficient.

A survey by GAO found that industry estimates between \$15,000 to \$100,000 per switch. Given 20,000 switches in use in the domestic local exchange and interexchange industries, 1,100 switches in the wireless industry, and even assuming that the actual costs are in the midpoint of the range would place retrofitting costs of about \$1.2 billion, 2½ times the amount authorized by the bill. Who bears the risk if retrofitting costs are inaccurate?

In addition to the costs associated with retrofitting, there are costs involved with new equipment, and it is not clear, as you heard this morning, that such costs would be de minimis. Such presumptions are based on assumptions that single hardware-software solutions can be applied in all cases. Technical requirements can and often do vary widely from one carrier to another and a hardware-software solution that applies in one instance may not apply in another.

Since it is uncertain what requirements are required now and in the future, it is difficult to project what type of technological solutions may be appropriate and what the cost of these solutions should be. Until more information is available, there is no substantive reason to justify any statement that the cost of future compliance will be de minimis.

Thank you for allowing TIA to testify.

Mr. MARKEY. I thank you, Mr. Bart, very much.

[The prepared statement of Daniel L. Bart follows:]

STATEMENT OF DANIEL L. BART, VICE PRESIDENT, TECHNICAL AND REGULATORY AFFAIRS, TELECOMMUNICATIONS INDUSTRY ASSOCIATION

The Telecommunications Industry Association (TIA), which represents more than 550 U.S. manufacturers of telecommunications equipment, is pleased to have this opportunity to comment on the manufacturing provisions of H.R. 4922, and on the financial implications of the digital telephony issue.

As an initial matter, the TIA believes that H.R. 4922 is the product of a lengthy and reasoned discussion between congressional, law enforcement, and telecommunications industry interests, and in the view of the TIA, the bill represents a significant improvement over FBI Digital Telephony proposals circulated in 1992 and February 1994. Accordingly, while the TIA strongly prefers continued efforts to foster cooperation¹ between law enforcement authorities and manufacturers of telecommunications equipment, the TIA believes that further refinement of H.R. 4922 would yield legislation which will both accommodate the legitimate needs of the law enforcement community and adequately safeguard the interests of telecommunications equipment manufacturers.

While many of the TIA's concerns regarding the impact of this legislation on manufacturers were addressed during the negotiations which preceded the introduction

¹Such cooperation has been conducted in fora such as the Electronic Communications Service Provider (ECSP) Committee, which is sponsored by the Alliance for Telecommunications Industry Solutions (ATIS).

of H.R. 4922, there remain several manufacturing-related and financial issues that the TIA believes require the attention of the subcommittee.

The first matter of concern to the TIA is that of who defines what constitutes a "reasonable charge" for equipment modifications required under subsection 2605(b). Historically, the price that manufacturers of transmission and switching equipment charge for their products has been determined by market forces, and the price of such equipment traditionally has not been regulated. This reliance on market forces has created a robustly competitive market for the manufacture and sale of telecommunications transmission and switching equipment, and it has encouraged technological innovation by those involved in the manufacturing process.

The subcommittee should seek to ensure that the present reliance on market forces is not disturbed, and thus should take care, in subsection 2605(b), to explain that it is not the subcommittee's intent for the Federal Communications Commission, or any other agency of the Federal Government, to regulate the price of telecommunications transmission and switching equipment. The TIA regards regulation as unnecessary in what is a truly competitive marketplace, and asks the subcommittee to clarify that determinations regarding what constitutes a "reasonable charge" for modifications should be made by manufacturers, in consultation with their customers, in accordance with normal and accepted business practices.

Additionally, the TIA urges the subcommittee to clarify subsection 2605(b) to clearly indicate that when a manufacturer undertakes "such modifications as are necessary to permit" its customer, i.e., a telecommunications carrier, to comply with the requirements of H.R. 4922, the manufacturer is to be paid by the telecommunications carrier, in accordance with normal and accepted business practices. This clarification is important because while a telecommunications carrier can recover the cost of its compliance from the Federal Government or its ratepayers, a manufacturer of transmission and switching equipment has only a single source—its customers—from which it may seek compensation for such costs.

The second matter of concern to the TIA is the possibility that manufacturers will face civil penalties if they fail to comply with the requirements of H.R. 4922.

Under normal business practices, telecommunications carriers set forth technical requirements (in a procurement procedure known as a request for quotation or RFQ) when they contract for equipment. The provisions of H.R. 4922 are consistent with this practice, as, in accordance with subsection 2605(a), telecommunications carriers would communicate to their preferred or chosen manufacturer what type of modifications, i.e., intercept capabilities, may be necessary. After such communication, the manufacturer would be compelled, by its existing contract (and, presumably, by its desire to secure future contracts), to provide whatever modifications might be required. The TIA acknowledges and appreciates the bill's reliance upon the existing and accepted process for procurement.

The TIA is much less comfortable, however, with the provisions of subsection 2607(f), that would subject a manufacturer which fails to provide the necessary modifications to a civil penalty of up to \$10,000 per day for each day such manufacturer is not in compliance with the requirements of H.R. 4922. While the imposition of civil penalties may be appropriate with respect to telecommunications carriers which fail to comply with the requirements imposed by H.R. 4922, in that there is no marketplace mechanism to ensure compliance by telecommunications carriers, there is no need to apply such significant penalties to manufacturers, as there is an existing marketplace mechanism to ensure manufacturer compliance.

In the event that a manufacturer fails to comply with the requirements of H.R. 4922, said manufacturer will face significant risk of a breach of contract suit brought by any telecommunications carrier which employs said manufacturer's equipment and is, therefore, unable to comply with the requirements set out for telecommunications carriers. Given the likely severity of the civil and marketplace sanctions that would accompany a breach of contract suit, the TIA believes that market considerations will adequately ensure manufacturer compliance. Accordingly, the TIA considers the imposition of civil penalties on manufacturers to be both totally unnecessary and counter to the cooperative spirit embodied in H.R. 4922.

The third issue with which TIA is concerned is that of when the Federal Communications Commission (Commission) may involve itself in the standards-setting process. Under subsection 2606(b), the Commission is authorized to set standards when private sector standards-setting bodies fail to do so, or if "a government agency or any other person believes that such standards are deficient." This is a very broad grant, in that it requires neither a specified time period within which private sector bodies are allowed to perform these activities prior to Commission involvement, nor any demonstrable showing that a standard is in fact deficient.

The TIA, which serves as a major contributor to the considerable volume of volunteer standards that promote trade and commerce in telecommunications products, urges the subcommittee to clarify subsection 2606(b) to require that private sector bodies have a reasonable opportunity to act prior to any commission involvement in the standards-setting process. The TIA also asks the subcommittee to strengthen the criteria which an agency or individual challenging a standard must meet in order to compel commission involvement in the standards-setting process. Accordingly, the TIA recommends that an agency or individual which challenges a standard be required to make an objective showing that the standard in question is deficient.

The final issue of concern to the TIA is cost. Although congressional, law enforcement, and telecommunications industry interests made significant progress toward resolving the broad policy issues included in H.R. 4922 prior to its introduction, the matter of cost remains unsettled.

To a great extent, capability and capacity specifications will determine costs, and until the law enforcement community makes clear its expectations for such requirements, all cost estimates are highly speculative. Nevertheless, while it is difficult at this juncture to accurately estimate the cost associated with compliance with the requirements of H.R. 4922, it is possible to identify a range within which cost is likely to fall, and, on the basis of that information, to conclude that the \$500 million authorized by the bill may be insufficient.

A recent survey by the General Accounting Office² found that industry estimates for retrofitting existing switches ranged from \$15,000 to \$100,000 per switch, depending on the complexity of the hardware and software modifications involved. Given that there are presently approximately 20,000 switches in use in the domestic local exchange and interexchange industries, the aforementioned estimates establish a range of between \$300 million and \$2 billion. Additionally, there are approximately 1,100 switches in use in the wireless industry, for which the cost of compliance may be estimated to be between \$16.5 million and \$110 million. Assuming that actual costs are at the mid-point of these ranges would place the cost of retrofitting existing equipment at \$1.21 billion, almost 2½ times the amount authorized by H.R. 4922.

In addition to the costs associated with retrofitting existing equipment, there are costs involved with building surveillance capability and capacity into new equipment, and, contrary to statements made by the Federal Bureau of Investigation, it is not clear that such costs would be de minimis.

The reason that presumptions regarding de minimis costs are erroneous is that such presumptions are based on the assumption that a single hardware or software solution can be applied in all cases. This assumption is false.

When a telecommunications carrier contracts to buy a switch, it sets forth technical requirements (as noted above) for such, and those technical requirements can, and often do, vary widely from one telecommunications carrier to another. Manufacturers customize their switches to meet the often disparate needs of their customers, and customization may dictate that a hardware or software solution which applies in one instance may not apply in another, depending on how a telecommunications carrier's switches are configured and deployed.

Because it is uncertain what type of requirements will be requested in the future, it is difficult to project both what type of technological solutions may be appropriate and what the cost of those solutions will be. Obviously, the former will have a significant impact on the latter, and until more information is available, there is no substantive reason to justify any statement that the cost of future compliance will be de minimis.

In sum, the TIA considers H.R. 4922 to be a significant improvement over previous legislation proposals regarding digital wiretap capabilities, and believes that with adequate attention devoted to the issues noted above, H.R. 4922 would yield legislation that will meet the legitimate needs of the law enforcement community and safeguard the interests of manufacturers of telecommunications equipment.

The TIA thanks the subcommittee for the opportunity to comment on this important legislation, and looks forward to working with the subcommittee's members and staff.

Mr. MARKEY. That completes the opening statements of our witnesses. We will now turn to questions from the subcommittee mem-

²GAO Testimony delivered before a joint hearing of the House Judiciary Subcommittee on Civil and Constitutional Rights and the Senate Judiciary Subcommittee on Technology and the Law, August 11, 1994, p. 5.

bers, and we will begin by recognizing the gentleman from Texas, Mr. Fields.

Mr. FIELDS. Mr. Neel, Mr. Wheeler, let me begin with you. You know, you heard the panel, first panel. You have got law enforcement basically coming to Congress in enmity saying, we must have this upgraded capability. I have just heard this panel say that we are willing to work with law enforcement, so that says to me that somewhere there is a consensus. Where is that consensus?

Mr. WHEELER. Well, I think the consensus is in the fact that, yes, it makes sense to update the laws to deal with new technologies. I think that where the consensus begins to fall apart is, OK, now how are you going to pay for that? And that, as I tried to say, in the ongoing negotiations with the FBI, they have moved from a bill which really didn't understand how, for instance, wireless telecommunications works and had some, therefore, provisions that didn't make any sense, to drafting a bill that is implementable, if there is such a word.

The problem is how are we going to pay for that, both in the short term and the long term? Because the discussion here this morning has obviously gone back to the point, as Mr. Neel said, there ain't no such thing as a free lunch.

Mr. NEEL. The consensus is really that law enforcement should be able to continue to wiretap these new digital services, in effect. It is not digital technology that is not wiretappable; it is the kinds of new services that simply go beyond your grandfather's network where you could take two little alligator clips and tap into a conversation.

It seems to me that what has happened is that the government has essentially thrown up its hands and said, we can't figure out how to deal with these new flows of data and information that are digital in nature, and there are these new services that have become very popular, and they represent a potential threat. So instead of saying, let's figure out how to fix this and spend enough money to fix it so we can continue to gain access, let's shift the accountability, the responsibility for this problem to, in this case, telecommunications carriers, which is something of a change.

The real issue here is, why do we need legislation? I am not sure we need legislation to mandate the wiretapping capability. We may need—we probably need legislation to appropriate the funds to allow law enforcement to buy the capability it needs, the capacity it needs and so on. It seems to me the real disagreement now, because both sides have made some concessions, is what is going to be paid for and how long will it be paid for.

Mr. FIELDS. Well, since both of you are saying to get to that consensus we have to deal with the question of cost—that is basically what we have talked about this morning—could you walk, both of you walk through with me in a simple sense, you know, what it takes to upgrade technologically, you know, giving an idea of the cost of that?

Mr. NEEL. Well, there may be others that could do this better. I can give you one sense that has relevance here.

Up until a few years ago, it was the sort of gentle evolution. It went from magnetic switches to digital switches and so on. And now you are moving into these new kinds of applications with fiber

technology and so on. But what has thrown a curve ball here is employing these new services that consumers want—call forwarding, speed dialing and so on—that require all kinds of changes in a network, in some cases, the taking out of an entire switch.

There are about 20,000 telephone switches in this country. When you have to take one out and put a new one in, the new one is going to cost a lot more. But you may have to do it to be able to provide these kinds of services to your consumers.

It is particularly a hardship in small telephone exchanges in rural areas where those costs may be the same per switch as they are for Southwestern Bell or whatever. So there are some costs that everyone has to bear, no matter how big their company is and so on. The economies of scale only go so far in this area.

So you may have to pull out a switch. You may have to design from scratch a whole new computer software regime to allow you to sell this service to your consumers. It is not a simple thing.

And I would imagine Tom would tell you when you get into wireless technology it is even more complicated.

Mr. WHEELER. Actually, it is probably a little simpler.

Mr. NEEL. Oh, good.

Mr. WHEELER. Because we have the advantage that you don't, Roy, of having a 10-year-old network versus a 100-year-old network.

So there are basically two things that you have to look at, Mr. Fields. One is the question of capability. The other is the question of capacity. Capability means, can you get the call detail information, the number from which the call is being placed or the number to which the call is being placed, and the ability to listen in, if authorized.

And the second issue, capacity, is do you have enough places to plug into the switch to get that? Because you need a port; to use computer terminology, you need a port for every tap you want to make. So what has to happen in a wireless environment is that you have to upgrade the switch to have the capability, because not all switches have the capability of having a pen register or getting the call detail information, and then you have to make sure that there are enough places where you can access that capability. And that is a two-step process, the first one being mostly software, and the second one being principally hardware.

Mr. FIELDS. One last comment, and I may come back and have additional questions.

It is not clear to me—again, looking at this from a cost perspective—that if this were phased in over a period of time—I do believe that both you and our previous panel addressed the regionalization of this issue. That is not something we should really consider. That doesn't really respond to the problem.

As much technological development and deployment as we see in the telecommunications industry, and also going back to the conversations I had with law enforcement in Houston, I guess I would like to know how much of the problem could be solved over a short period of time as things are replaced and in that replacement you build in the capability so that you actually get some economies of scale and hopefully have an impact on that cost going down?

Mr. WHEELER. Unfortunately, it is not—

Mr. FIELDS. That is really not a question. It is more of a statement, unless you want to respond.

Mr. WHEELER. The problem is, there is a trickle-down theory, if you will—particularly in our business, where we are constantly adding cell sites and switches, what you do is you go to the big market and as it outgrows its equipment, that equipment is replaced and goes down to a smaller market. The new equipment may be fixed, if you will, to solve the problem. You are still stuck with this switch here, and what are you going to do to upgrade it both with software and hardware?

Mr. NEEL. I think the problem, too, is that we just don't even know what kinds of new services could be developed, so the trade-off is in retarding the deployment of new services so you would have predictability in the network, fix the problem in front of you right now, perhaps gain some economies of scale over a short period of time.

But it ignores the kinds of new services that may come on line. The legislation exempts the Internet, CompuServe, America Online and those kinds of things. It does so potentially for political reasons, to not weigh down the bill. But also that is an area of enormous growth. Fifteen years ago, 10 years ago, no one would have predicted those kinds of things or even call forwarding, caller ID and all these things.

So the problem comes in taking a snapshot, fixing the network at the point you take that snapshot and assuming that that will hold for a considerable period of time, certainly beyond years. And we just don't have that assurance or don't have any reason to believe that that can be done.

Mr. FIELDS. Well, just in closing, it doesn't escape the subcommittee that there has been extraordinary cooperation and effort by the telecommunications industry, and again, it is my hope that this subcommittee will take a long, hard look at this particular issue and that, as this issue proceeds in Congress, that we get the sequential jurisdiction so that we can address these issues.

Mr. MARKEY. The gentleman's time has expired.

The Chair will recognize himself at this point for a round of questions. Let me get to a point raised by Director Freeh of the FBI earlier in his testimony. That is that this whole discussion about prioritization really doesn't take you too far because, from his perspective, the real costs are in the development and the R&D. And at the point at which you are trying to deploy it in Broken Arrow, Oklahoma, economies of scale have kicked in, and as you have finished L.A. and Boston and New York and Houston, the software and the other technologies have now been reduced in cost dramatically.

Is he correct in that assessment, Mr. Neel, Mr. Wheeler? Could you tell us how you view his analysis of the deployment issue as it hits the more rural areas of the country?

Mr. NEEL. Well, let me come to the snapshot metaphor here.

It may be true for one service, one time; at a point in time, you fix that, and you might be able to deploy that through the entire national network. But it doesn't do anything about the snapshot you may have to take 2, 3, 4, 5 years from now, or on a different kind of service, on a given day.

I wouldn't go so far as to characterize the Director's optimism as wishful thinking, because he may be right. And the example you used for captioning, the caption chip on television is correct insofar as it goes. But it may very well be—and we found it, for instance, in call forwarding—that these fixes are not necessarily transferable. And it is almost certain that the fix to make a service wiretappable on one kind of service is almost certainly not going to work on another kind of service.

And so if you just—

Mr. MARKEY. Just so I understand, let's take an example. Let's take Houston. You do Houston and now you have to go out 100 miles. What is the difference in terms of now applying the software that you have developed in a rural setting, with that telephone company, as opposed to in downtown Houston?

Mr. NEEL. First of all, you don't just plug new software that Southwestern Bell has in downtown Houston or that SouthCap has into a rural telephone system in rural Texas because he may not have the capability of doing that. He may have to completely pull out that switch and put in a new kind of switch to be able to do that, or he may not be allowed to deploy that new service, whatever it is. And his costs will be per switch about the same as they will be for the Southwestern Bell switch in downtown Houston.

Mr. MARKEY. So part of your objection then, or concern, is the size of the company itself and their ability to absorb these costs, since they don't have the critical mass of customers that the Southwestern Bell Company would have.

Mr. NEEL. Well, that is certainly a concern if that company were facing a mandate, unfunded, potentially, and severe civil penalties. But there is another aspect which is just the simple community relations issues.

A telephone company is going to want to be a good local citizen. They are not going to tell law enforcement, we are not going to do that for you until you pay us. They have traditionally not done that. There have been a lot of cases where a telephone company spent a lot of money—\$2, \$3 million dollars—and had to fight to get it back, in fact, wrote it off. They are going to want to, as Tom said, salute the flag and deliver the services.

So it is a combination of things. If those companies are reimbursed, if there is a true reasonable cost attached to this and if it is enforceable, then the objections begin to diminish.

Mr. MARKEY. Well, Mr. Wheeler, again, you don't have a 100-year-old infrastructure the way Mr. Neel does in many instances.

Mr. WHEELER. I can be real specific on that with you, Mr. Chairman. Of the 1,200 or 1,100 cellular switches in the U.S. today, there are probably 100 of them that are not upgradable, period. I mean, they are too small, too early in the generation of the trickle-down theory, as I talked about, and you have got to replace them, period.

Of the other, slightly greater than 90 percent of the switches, probably about 25 percent of those from one specific manufacturer don't have currently an upgrade path. The others do.

We are here, however, today saying that, yes, Congress should mandate this requirement on all wireless carriers, even though these problems exist and they are pretty serious problems. But I

am constrained to respond to one of the things that Mr. Bart said in his testimony, and that is that this is a team effort, that if they don't build it, we can't deliver it. And we don't want to be in a situation where the only person whose liability is hanging out there on the line is ours.

Mr. MARKEY. OK.

Mr. WHEELER. And there is 25 percent of the switches for which there is no software.

Mr. MARKEY. They have passed legislation in the House, they are going to pass it in the Senate, and we are going to put a bill on the President's desk in the middle of October for his signature. Isn't that right, Mr. Neel?

Mr. NEEL. I was just knocking on wood.

Mr. MARKEY. And in that legislation, we are going to allow telephone companies to provide cable service and cable companies to provide telephone service, et cetera, et cetera, giving each company a tremendous incentive to upgrade to the digital era in a very short period of time or risk their competitor's upgrading and taking real advantage of the inferior technology that the other company has.

Now, as each company begins to install the very modern equipment, which they are going to have to invest in if they want to move to this new era, how much added cost at that stage, where they are going to not just renovate but dispose of and move on to the new era, how much additional cost will it be for those companies which we believe to be the vast bulk in terms of the population served.

We understand that there is always going to be this 10 percent in the most rural part of the country. But for the 90 percent that is served primarily by the urban and suburban telephone services who will be pressed tremendously to upgrade technologically, why don't they have essentially incremental costs, since they are going to be making a lot of the, as you said—did you call it the "upgrade path?"

Mr. WHEELER. Right. Terms the upgrade path, of course, being much more difficult if you are going to be working off 30- or 40- or 50-year-old switching technology.

Mr. MARKEY. But if you are moving to this new era just to survive, why wouldn't the cost be marginal rather than geometric?

Mr. WHEELER. Here is the problem. The question and the direction of your question is on target. The problem is you can't answer it because we don't know the specifics that are going to be required. You are saying how much is it going to cost? I have no idea.

Mr. MARKEY. I guess what I am saying to you is, I am just getting back to this television analogy again. When you go from black and white to color, you are no longer talking about just improving marginally, and there are all the additional costs—on a black and white set. You, on the other hand, are going to have a brand-new technology that is going into people's homes, and as a result, if you want to add other things at that juncture, it is clearly not going to be as costly as if you try to go into a black and white TV set and have it do tricks that a black and white TV set was never intended to do. That is my only point.

As they move to digital and they do it on a more ubiquitous basis, just from a competitive perspective—again, I am trying to

use this closed-captioning chip analogy—why isn't it a relatively more simple thing to do than going back to the older systems?

Mr. WHEELER. Theoretically, you are correct, and we are not going to sell you what UHF or closed-captioning—we are not going to give you that kind of head-in-the-sand answer. The problem is, we don't know. How many ports should you have—24, 48, 6? Got no idea.

And do you know what, Mr. Chairman? In the bill, there is no procedure for establishing that other than the FBI, I am sorry, the Attorney General saying, this is the way it will be, we will "consult" in an informal proceeding where you have de minimis rights, and then we will unilaterally say that is what we want. And that is the problem.

Mr. MARKEY. All right. I see what you are saying. It is opened—

Mr. WHEELER. Right.

Mr. MARKEY. [continuing] from your perspective in terms of what the requirements would be.

On the other hand, in the generic question of degree of difficulty in implementing this new set of requirements in a competitor's system, as it is being newly designed in 1995 for deployment in 1997 or 1998 in order to be competitive in a community, it just seems to me that apart from the question of how many ports or how many wiretaps might be logistically capable of being done simultaneously to reduce dramatically the cost that will be added to the system. Let me go back to Mr. Neel.

Mr. NEEL. Mr. Chairman, the problem here is that what law enforcement wants, what the FBI wants here, is not something that would in any way be built into a network anyway. There is no benefit to the telephone company or the cellular company or the cable company, if it is in the local telephony, to derive from putting in that capability or that capacity for that matter. There is no incentive to gold plate here because this is not something that you can sell, that you can recover your costs in any other way.

The two technological evolutions here, one, to provide consumers what they now want with new services to build out the information superhighway and so on, is one path used. The fix to take care of wiretapping, all that stuff, is a whole other technological development. They are not, while they may be parallel in time lines, they do not necessarily complement each other, and in fact, the very evolution of more sophisticated digital services and technology complicates the other.

When Mr. Freeh said that I had noted or admitted that this does frustrate law enforcement's effort, the fact is it does complicate it because it is a new generation of services that are not easily tapped right now. But the two things are not joined, and so that is the reason you don't necessarily enjoy these huge economies of scale that you are suggesting. You have to do a whole new thing over here.

Mr. MARKEY. Mr. Berman.

Mr. BERMAN. I just want to come back to the point that I have listened to this debate in our coalition with the administration for 3 years, and no one has answered this question—it seems to me that the answer comes down to who bears the risk.

The government is prepared to bet the house that the costs are de minimis, that eventually it is like the chip in the TV, it just gets absorbed into the system. If that is true, then the taxpayer has no burden, no big burden coming up.

But if it is not true and the costs are substantial, then I think that, in terms of public accountability and balancing law enforcement and privacy and other values, you need to have this above board to pay for it, and it is also important to realize that we are trying to stay as close to the current law as possible.

Many of us have been brought kicking and, you know, screaming into this room because of the potential downside for technology for privacy. Under the current law, section 2518, when the government gets cooperation from industry or from landlords or from any of us to conduct a wiretap, they reimburse, they pay the necessary costs of that, so why not continue that tradition into the future?

Government pays the costs of that, and if they are de minimis, they are de minimis. If they are substantial, the taxpayer gets to decide whether they are prepared to foot the bill for law enforcement and impose an above the board wiretap tax on all consumers.

Mr. MARKEY. I appreciate that. I also appreciate, Mr. Berman, your efforts in helping to broker a compromise on this legislation.

The Electronic Frontier Foundation has been very valuable in this whole discussion, and reading Wired magazine each month, I realize how much criticism you can come under from those on the other side of the issue that even wonder why there is any cooperation at all with the government on these issues. So it is a fine line that each party has to walk on on each one of these.

Mr. BERMAN. Let me just respond.

Mr. MARKEY. If you could just briefly, then I want to recognize Mr. Boucher. Just expand for us upon the point which you made about how important it is to pass legislation so that there is expanded protection for telephone, electronic devise users in our country.

Mr. BERMAN. Absolutely. We came to the point where we understood that the FBI was saying this was a drop-dead issue for them, and while we could still have qualms about that side of the legislation, we also recognize that if we are going to take care of law enforcement on the one side, why don't we address some of the open-ended questions about privacy that are created by new digital technologies.

I mean, the world didn't stop in 1986 with the Electronic Communications Privacy Act, and one of the pressing issues is the enormous amount of transactional information that is being generated by and about us in conducting our lives on these electronic networks.

The E-mail analogy to regular mail is just not apropos. As you know, for using E-mail, it becomes a minute-by-minute portrait of who you are talking with, what you are doing, what you are negotiating back and forth, so that even the address line which says to and from reveals content about communications, and so we are creating a new court order in this legislation; Congress is creating a new court order for the transactional information in electronic mail, which I think is an important new protection. It breaks the line between transaction and content and says that we are—that

line is blurring, and so we think that when all the dust settles, and if we can work out the mechanics of the law enforcement side, that there are privacy gains to be won here.

It is also important that pen registers, which now pick up more information than simply the dialed number, because you are using that touch-tone phone to do a lot of different banking, and other kinds of transactions—that the FBI has to move towards technology which does not capture anything except the dialed number.

The O.J. Simpson case—maybe there was a probable cause and a warrant to track where he was going with his cellular phone that day, but the capability of tracking anyone under suspicion in this country using this technology is a real one, and this legislation says you cannot design that into the technology.

And one of the great fears of letting the FBI design the system is that they would provide for remote wiretap where they would be able to turn on the system at the central switch somewhere in a remote location. Congressman Edwards and Senator Leahy have made it clear that that is not possible. You need human intervention.

So some of the fears that we have have been taken care of in this legislation, and in the end, I think, we are bringing a process of cooperation, which is going on between law enforcement and industry, not behind closed doors, but in the public realm where they are trying to decide how to meet requirements, into the above board public realm so we can make some public judgments about what kind of design network we are going to have.

Mr. MARKEY. I appreciate your point, Mr. Berman. It is very well made, so that on the one hand, we are giving, in this legislation, considerable benefits to the FBI, but it is towards the goal of insuring that they are able to keep their existing powers in a new technological realm. While you are also making the point that the laws of our country have yet to, in fact, deal with the need to give protections to people who are using these new technologies, whether it be E-mail or cellular phones, and that this legislation is giving us an opportunity to give protections to people in their homes, in their businesses, against unwanted and unjustified intrusions into their privacy without court order. And I think that balance is one that people don't understand in terms of the way in which the legislation is constructed.

Mr. BERMAN. It just takes us beyond the legislation of 1986. So many things have changed that this gives us a chance to make some upgrades in privacy.

Mr. MARKEY. Thank you very much. That completes my time.

I have to now recognize the gentleman from Ohio, Mr. Oxley. I apologize to the gentleman from Virginia. The gentleman from Ohio.

Mr. OXLEY. I thank the Chair. You didn't really have to, but I appreciate that courtesy anyway, Mr. Chairman.

Let me ask Mr. Wheeler, today it is relatively easy for someone to essentially tap wireless service. As a matter of fact, we had a demonstration here in this very committee room a year or so ago where a young man went down and bought a Radio Shack scanner and essentially turned it into a—we picked up traffic from the room. Obviously that is illegal. I wonder—

Mr. WHEELER. Interestingly enough, Mr. Oxley, it is only recently, only since the last session of the last Congress, that the ownership of the equipment to do that or the sale of the equipment to do that has been illegal. There are now 12 million units out there that can do that legally today.

Mr. OXLEY. I do remember that. Counsel reminds me of the authorization bill.

If you can, what is the difference then between—other than a court order from a law enforcement—request from law enforcement, a court order from a magistrate or a judge, there is literally no difference in the ability to pick up wireless conversations except one is illegal and one is not; is that correct?

Mr. WHEELER. What we are talking about is really intercepting at two different points. One is while the conversation is in the ether, and that is what the scanners do, and it is very difficult to say, "I want to listen to Mr. Oxley's conversation", because it has to scan across multiple channels, and the odds of picking you up are thereby slim, but you can be picked up.

Then what this bill deals with is once you get inside the telecommunications system, if you will, you have gone to the cell site, you are going down into the switch, we want to pick up your conversation, law enforcement wants to pick up your conversation and your conversation alone, so it is really two different technical opportunities, and I might add that in the former opportunity, that is being increasingly thwarted by the introduction of new digital technology coupled with what the Congress did to make it illegal to sell the equipment to eavesdrop.

Mr. OXLEY. I appreciate that. That is a distinction I think that is important, and I am glad you brought that out because I had some problems with that myself.

Let me ask both you, Mr. Neel, if you were in our position and looking at, I think, the inevitability of legislation in this area, that is, the upgrading of the technical ability of law enforcement to continue to wiretap with new technology, and given the fact that the cost clearly is the major stumbling block here, and even if the figure turns out to be more than was anticipated, how would you suggest that we—or that society pay for this kind of technology to allow that to occur?

Mr. WHEELER. Well, I think there are two parts to the question. One is, what is to be required, and the second then is who writes the check.

And again, I go back to the fact that what this bill doesn't do is to say what is to be required or what the procedure is and to establish procedural safeguards so that the public accountability, Mr. Boucher, is there. So that will have the effect of differentiating between wants and needs, if you will. OK. So now we are down to needs. Let's assume that gets addressed.

Now, we are down to needs. I mean, I agree with Director Freeh. He said before the Judiciary Committee, because there is such a great national and Federal interest here, both national security and criminal, it really does seem appropriate to me that the Federal Government bear the costs. I think that is a legitimate statement that he has made.

Mr. OXLEY. Mr. Neel.

Mr. NEEL. Well, I think first of all I would urge you to apply this to all providers so it is competitively neutral, so you don't open up a whole new incentive for providers that don't have to comply.

I would limit the mandate to services within the capacity and capability of law enforcement, the government, to pay for, primarily to insure accountability, and either take off the cap of 4 to 6 years on willingness to reimburse for capability or sunset the entire law after 4 to 6 years and revisit it and see how much more money you may need to do that.

Mr. OXLEY. I appreciate that.

Mr. Berman, did you have a comment?

Mr. BERMAN. No.

Mr. OXLEY. Mr. Bart.

Mr. BERMAN. We are back to the cost issue.

Mr. BART. I think Congress provided the right balance under the current law, under section 2518. The current law says government pays. We think that should be maintained.

Mr. OXLEY. Let me just go back to Mr. Neel before I complete, Mr. Chairman.

You are talking about a pay as you go kind of a concept then?

Mr. NEEL. In effect, yes.

Mr. OXLEY. And that would be a phase in of the most—the most need, as Mr. Wheeler pointed out to begin with, so we look at the New Yorks and the Chicagos and the Bostons first and then cost it out?

Mr. NEEL. Well, that would be up to the government and law enforcement. If it had so much money it could spend, I would assume it would set those priorities.

Mr. OXLEY. So from your perspective, it would be dictated by the amount authorized and appropriated.

Mr. NEEL. Yes, because essentially that is the only way you maintain that accountability.

Mr. OXLEY. I thank the panel. It has been most enlightening.

Thank you, Mr. Chairman.

Mr. BOUCHER [presiding]. The gentleman's time has expired.

Mr. Bart, I would like to take just a few minutes to draw on your expertise with regard to telecommunications equipment and the costs that we could anticipate being required in order to make the kinds of modifications that have been discussed here today.

We tend to think of these costs as being separated into two time frames. The first of these is the transition phase of the first 4 years where it is generally understood that the government will bear those costs, although there are some questions as to how precisely that has been drafted, and then a second time frame that is the post 4-year period in which the burden will be on the industry to carry further cost of modification.

You indicated in your statement a few minutes ago something that I thought was very revealing, and that is that you estimate the mid-range of the estimated cost for modification to be about \$1.2 billion, whereas the government's responsibility at the outset would be limited to a maximum of \$500 million.

So just taking those figures alone and realizing that the \$1.2 billion is only the mid-range, that the costs could be greater than that, we could be looking at very substantial costs, in fact, being

imposed on the industry, not the kinds of de minimis charges that Mr. Freeh and others think would result.

Would you care to comment on that and elaborate some as to that \$1.2 billion figure? And also, if you would, tell us if that figure would be incurred in the first 4-year period or if you were looking at a \$1.2 billion figure stretched over a longer time frame.

Mr. BART. The figure was derived from taking the GAO estimates, which I believe they had talked to various manufacturers and service providers and provided a range per switch, and I think as everybody has testified to, all the estimates are highly speculative because we don't know precisely what the capabilities and the capacity issues are. However, for our testimony, we said even assuming that there will be some high and some low, we are looking at a mid-range, which I think was \$57,500 per switch, and apply that to the 20,000 switches that are in the local exchange, inter-exchange networks, on the 1,100 switches that Tom has talked about in the wireless network; you derive that \$1.2 billion figure.

In looking at Mr. Wheeler's testimony, I noticed on page 11 that he said that the average cost for such capability was \$50,000 and the couple switches that were upgraded and part of the capability, so \$57,000 was very close to the \$50,000 that Tom has put in there, but I think it depends on each switch.

Each switch is different. Chairman Markey said, if I do it for Houston, is that the same thing I need to do for Broken Arrow Oklahoma? I think the answer is no. Houston may have a big switch provided by one carrier where Broken Arrow Oklahoma may have a different switch from a different manufacturer. The switch in Houston may have ISDN and other complex features. The one in Broken Arrow, Oklahoma may not.

So each switch, each customer's requirements are unique. The manufacturer has to look at what is the switch type, what is the feature that particular customer is using, is there an upgrade path, as Tom said, or is the upgrade path basically saying the conversion—you throw that switch away and put a new one in.

People see this with their personal computers. There are certain things you can do to a 286 to add, but at a point in time, you throw the 286 away and you put in a 486 because you have exceeded the capabilities. And the upgrade itself is a whole new switch. The same thing applies in the public switch network.

Mr. BOUCHER. During what time frame would you anticipate this \$1.2 billion cost being incurred? Is that just the first 4 years?

Mr. BART. That was the retrofit figure, as I understood it, from the GAO estimate.

Mr. BOUCHER. Just for the first 4 years. And then if you would separately address the question of long-term costs. Mr. Freeh, when he testified, admitted to the possibility that there could be substantial long-term costs, post first 4-year costs.

What is your thinking on that subject? Do you agree that they could be substantial and would you care to assign any dollar amounts to what those costs might be?

Mr. BART. We do believe that they could be substantial. We are dealing with the unknown. We don't know what the unknowns are. A cellular carrier could provide a \$50,000 upgrade today only to find out, as Tom Wheeler has testified to, that that gave you the

capacity and the capability, but mousetraps breed smarter mice. The crooks are now cloning the phones, so after having spent \$50,000, we are still not wiretappable because the crooks are doing something else. That can come back by way of new capability requirements for switch manufacturers.

Now, what can you do to catch the guy who is cloning the phone? Is there anything else you can do other than make the phone illegal? You go back to the drawing board, and say, there is a new set of capability requirements, can we redesign those? Once we redesign them, we can now deploy them and that triggers the capacities.

We think the costs could be substantial, but at this time we don't know what they are. New features are invented on the network every day, significant costs are being spent every day just to keep the SS7 networks and other ones up to date. Each one of those new capabilities would trigger a new capability set on the wiretap.

Mr. BOUCHER. Well, does that uncertainty then suggest that what Mr. Neel had mentioned and a couple of other witnesses parenthetically commented on should be given serious consideration, and that is, potentially a sunset of this requirement after the initial 4-year period with a clear opportunity then at the end of that time for Congress to look at the state of technological advance, to evaluate the kinds of new services that are then being introduced and are anticipated to be introduced in the future, and then have a better sense of what the costs might be before deciding how those costs are going to be borne or in fact if they should be borne at all. Is that an idea that we should seriously examine? And I would invite others to comment if they choose. Mr. Bart.

Mr. BART. That is one approach. The other approach would be to shift the so-called de minimis threshold over to the government to say, whatever they are, put it through the normal government appropriations cycle. This is another approach that would take a fresh look.

What we are opposing is the assumption that because the costs are de minimis, shift them to the industry. If they are de minimis, people could say it is irrelevant who bears them. But we have the feeling that because of the push on the industry side, that some people believe they won't be de minimis and want somebody else to absorb that cost.

Mr. BOUCHER. Anyone else care to comment? No.

Mr. Neel, let me ask you one question, and that is this: If the legislation passes in its current form, and assuming the correctness of Mr. Bart's figures, industry would be required to bear some very substantial costs, about \$700 million just through rough calculations.

Would that, in your opinion, possibly retard the introduction of new technologies? Does it have the potential to delay the deployment of the advanced information infrastructure that it has been one of the principal objectives of this committee to advance and encourage during this Congress?

Mr. NEEL. I think it could retard deployment of technologies in two ways. One, it could simply send a message to carriers that they are not going to be able to recover costs potentially, so don't even consider putting this in place.

And the civil penalties that exist in this legislation would send another kind of signal to entrepreneurs and developers of new technologies that this is a very serious problem, why do we want to undertake this, let's invest in something else. So for some of the kinds of services that could potentially create a problem, even though there is no certainty, it could drive investment in other directions. It could be a damper on the deployment of new technologies.

Mr. BOUCHER. Great. Mr. Wheeler, would you care to comment?

Mr. WHEELER. Yes, and may I also, Mr. Boucher, comment that we are here representing not just the cellular industry, but also the ESFR companies such as Nextel and the PCS license holders, soon to be license holders, and let's look specifically at those last two for a second because they are the new competitors in the wireless world.

They are looking at the raw undeveloped spectrum to be able to provide new competitive services, and it is a very capital intensive exercise to do that, and we are increasing the cost of the capital. Clearly that has to have an impact.

Mr. BOUCHER. My time has expired. I will recognize again the gentleman from Texas, Mr. Fields.

Mr. FIELDS. Just a very quick question. As I was sitting here thinking about this, I was thinking about some of the things we are talking about as an inverted pyramid, capacity, capability, and of course cost, and Mr. Wheeler, you are the one who really made me stop and think about this capacity, capability problem.

I guess, like many other members, I invoked this primarily on cost. But when you look at section 9 of the bill and you realize that the Attorney General is the one making the decision on capacity and capability, that in itself could also be an issue that we really need to address.

How would you construct someone setting or some group or entity setting a standard? I assume it would be someone in addition to the Attorney General. Certainly he is a key player.

Mr. WHEELER. I find it very interesting that on the capacity, I am sorry, the capability side of the equation, the bill is specific and it says that industry and law enforcement will try and work together and that there is, failing that, a structure at the FCC which is an on-the-record rulemaking where everybody comes in, presents their evidence, challenges the other guy's evidence and bangs away in the caldron of competitive ideas to come out with rulemaking, which is a—

Mr. FIELDS. Which is a normal—

Mr. WHEELER. [continuing] which is a normal course of action. That is what they do in the capability side of their responsibilities.

In the capacity side, it is, well, we will consult with you and then we will do whatever we please, and that causes great concern. I mean, we believe that there needs to be an on-the-record proceeding where there is the competition of ideas to help differentiate wants from needs and in which there are defined rights for the parties in the proceeding as well as to review the proceeding, and that if you can have that as a procedural mechanism, then you can begin to get your arms around, well, what exactly are the requirements going to be and only then can you know what the costs are going to be.

Mr. FIELDS. I appreciate that point. To me again that underscores the need for this subcommittee to take a long, hard look at this legislation and certainly have jurisdiction ourselves, because our perspective is not always the same as the Judiciary Committee.

Thank you, Mr. Chairman.

Mr. MARKEY [presiding]. The gentleman's time has expired and all time for questions from the subcommittee members has expired as well.

Let me ask each of you to give us a 1-minute summation of what it is that you want us to consider in this final 4 weeks or so of this session of Congress as we try to wrap up this legislation, try to be sure that we have done everything we could to deal with all the legitimate concerns of all the parties that are contesting this particular piece of legislation.

Let's go again in reverse order, 1 minute a piece, please. We will begin with you, Mr. Bart.

Mr. BART. Thank you. I believe today's hearing shows that cost is a major issue standing before the subcommittee. I would like to point out that in TI's testimony, we used a \$1.2 billion figure which was one-half of the GAO range for purposes of illustration that we don't believe the \$500 million is a good number; not because that is the actual number.

At this point we don't believe anybody knows what the actual number is because it depends upon the capability and capacity, a bunch of unknowns that we are struggling to grope with right now. I would not want to mislead the committee to think that \$1.2 billion is an actual number. We heard lots of testimony today. There is a lot more refinement that is necessary in the cost figures. Until we know what the real costs are, we need an accountable method to determine those costs and who should pay those costs.

Mr. MARKEY. Thank you, Mr. Bart, very much.

Mr. Wheeler.

Mr. WHEELER. Very quickly, we would support the legal wiretap capability being extended to new technologies, but in so doing, we need to have public accountability as to what those requirements are, and that means procedures. And second, we need to link compliance to reimbursement.

Mr. MARKEY. Thank you, Mr. Wheeler.

Mr. Berman.

Mr. BERMAN. I would just reiterate that I think this legislation can go as far as possible to strike a balance between law enforcement needs and privacy if we can resolve this cost issue and create a process where it is really on the public record and where costs are recoverable.

That is the way to ensure that we are not going into an era where the government would be dictating standards and using the bully pulpit which they have, which is law enforcement, to create great pressures on industry to move our technology in the wrong direction.

Mr. MARKEY. Thank you, Mr. Berman.

And you, Mr. Neel, you have the last word.

Mr. NEEL. I would just urge you to look back at the record you created when, in March, you decided to essentially blow up the rules that govern this environment and recognize that the future

network is where the problem is and that you should take into account that there are many different kinds of players. This is not an easy problem. Cost is the issue and that if the government orders services and products, it should be willing to pay for them. And that is a public good, that kind of accountability.

Mr. MARKEY. Thank you, Mr. Neel, very much. This whole discussion raises for this subcommittee the law of unintended consequences as we push the private sector to invest in new technologies, to compete with each other, to move us more quickly towards the digital era which will help to revolutionize our business, our education, our health care systems in this country and let us be the number one country in exporting these technologies around the world.

But at the same time, we don't want to have a back-door repeal of the 1968 Wire Tap Act. We don't want other things to happen that come as a necessary consequence of the upgrade of these technologies. I think we can work through a lot of the legal questions that have been raised and I think Congressman Edwards and Senator Leahy have done an excellent job towards that end.

The remaining questions, those of cost and which responsibilities should be placed upon common carriers, are a little bit more meddlesome, and I think that although there is some disagreement that we have elicited from the two panels today, it is still possible to be reconciled so that the objective of passing legislation and putting it on the President's desk this year can still be met, and with the cooperation of the witnesses on both panels, we can achieve that end.

We would like to work with you so that, in an expeditious fashion, we can resolve some of the issues and try to pass legislation to advance the goals which I think all of us seek to achieve. With that, this hearing is adjourned.

[Whereupon, at 2:03 p.m., the subcommittee was adjourned.]

[The following material was received for the record:]

ONE HUNDRED THIRD CONGRESS

- JOHN D. DINGELL, MICHIGAN, CHAIRMAN

HENRY A. WAXMAN, CALIFORNIA
 PHILIP R. SHARP, INDIANA
 EDWARD J. MARKEY, MASSACHUSETTS
 AL SWIFT, WASHINGTON
 CAROLISS COLLINS, ILLINOIS
 MIKE SYNAR, OKLAHOMA
 W. J. BILLY TAUZIN, LOUISIANA
 RON WYDEN, OREGON
 RALPH M. HALL, TEXAS
 BILL RICHARDSON, NEW MEXICO
 JIM SLATTERY, KANSAS
 JOHN ERYANT, TEXAS
 RICK ROUCHER, VIRGINIA
 JIM COOPER, TENNESSEE
 J. ROY ROWLAND, GEORGIA
 THOMAS J. MANTON, NEW YORK
 EDOLPHUS TOWNS, NEW YORK
 GERRY E. STUODS, MASSACHUSETTS
 RICHARD H. LEHMAN, CALIFORNIA
 FRANK PALLONE, JR., NEW JERSEY
 CRAIG A. WASHINGTON, TEXAS
 LYNN SCHENK, CALIFORNIA
 SHERROD BROWN, OHIO
 MIRE EREDLER, WASHINGTON
 MARJORIE MARGOLIS MEZVINSEY, PENNSYLVANIA
 BLANCHE M. LAMBERT, ARKANSAS

CARLOS J. MOORHEAD, CALIFORNIA
 THOMAS J. BILEY, JR., VIRGINIA
 JACK FIELOS, TEXAS
 MICHAEL G. ORLEY, OHIO
 MICHAEL BURRIS, FLORIDA
 DAN SCHAEFER, COLORADO
 JOE BARTON, TEXAS
 ALLE McMILLAN, NORTH CAROLINA
 J. DENNIS HASTERT, ILLINOIS
 FRED UPTON, MICHIGAN
 CLIFF STEARNS, FLORIDA
 BILL PAXON, NEW YORK
 PAUL E. GILLMOR, OHIO
 SCOTT ELLIG, WISCONSIN
 GARY A. FRANKS, CONNECTICUT
 JAMES C. GREENWOOD, PENNSYLVANIA
 MICHAEL C. CRAPO, IDAHO

ALAN J. ROTH, STAFF DIRECTOR AND CHIEF COUNSEL
 DENNIS B. FITZGERIBS, DEPUTY STAFF DIRECTOR

U.S. House of Representatives
Committee on Energy and Commerce
 Room 2125, Rayburn House Office Building
 Washington, DC 20515-6115

September 20, 1994

The Honorable Thomas S. Foley
 The Speaker
 U.S. House of Representatives
 H-204 The Capitol
 Washington, D.C. 20515

Dear Mr. Speaker:

I am writing with regard to H.R. 4922, a bill which regulates telecommunications carriers through the Criminal Code. I was distressed to see that this legislation was initially referred solely to the Committee on the Judiciary, particularly since the "regulation of interstate and foreign communications" is expressly within the jurisdiction of the Committee on Energy and Commerce under Rule X. I am writing to ask that you sequentially refer H.R. 4922 to this Committee for an extended period of time.

In April, 1993, I testified before the Joint Committee on the Organization of the Congress. In that testimony, I noted that

"when a committee decides it wants to "do" a particular issue, it starts designing bills to avoid the real committee of jurisdiction by drafting the subject matter into Acts in its own jurisdiction having no real relation to the subject matter. I don't permit this type of jurisdictional raid with respect to subcommittee referrals, and it should be prevented with respect to committees under the rules of the House."

It is clear to me that as long as this type of chicanery is rewarded by a referral to a sole committee, jurisdictional raids such as this will continue unabated.

While H.R. 4922 is motivated by legitimate law enforcement concerns, it is replete with regulatory solutions that have no business in the Criminal Code. Moreover, inasmuch as the legislation was drafted so as to obtain the desired referral, its

The Honorable Thomas S. Foley
Page 2

strange statutory placement is contrary to the dictates of good drafting.

Section 1 of H.R. 4922 adds a new Chapter 120 to Title 18. This new chapter imposes significant new regulatory requirements on a substantial number of telecommunications carriers, many of which appear to conflict with existing state and federal communications statutes.

For example, proposed section 2603 requires telecommunications carriers to ensure that they have sufficient capacity so as to be capable of complying with an estimate issued by the Attorney General. Yet the construction of telephone plant, including the acquisition of the necessary equipment, is regulated by the Federal Communications Commission (for plant used for interstate and foreign communications) and the 50 state public utility commissions (for plant used for intrastate communications). H.R. 4922 would thus give the Attorney General the ability to order regulated telecommunications carriers to construct and operate facilities that may not have been approved by either the Federal Communications Commission or the appropriate state public utility commission.

Proposed section 2605 extends -- for the first time -- federal regulation to the manufacturers of telecommunications equipment. And although this proposed section does not directly amend the Communications Act of 1934 (47 U.S.C. 151 et seq.), it nevertheless grants additional authorities and responsibilities to the Federal Communications Commission. For example, the Commission's involvement with industry standard-setting activities has historically been minimal. Section 2605 injects the Commission directly into that process for the first time.

Furthermore, several provisions of this section appear to conflict directly with the provisions of the Communications Act.

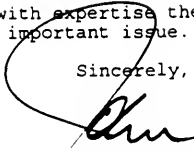
Proposed section 2608 purports to ensure that telecommunications carriers that are required to expend funds in order to comply with the dictates of the Attorney General are reimbursed for such expenditures. However, it is not clear that, if appropriated funds are insufficient to fully reimburse a carrier, regulatory agencies will be required to increase telephone rates, and ratepayers forced to bear the burden of compliance.

Mr. Speaker, it is clear that H.R. 4922 is a regulatory bill that falls within the jurisdiction of this Committee. Given the shortness of time that is remaining prior to adjournment, it is my hope that you will refer this bill sequentially to the Committee on Energy and Commerce for an extended period. To do otherwise would reward an effort to "game" the referral process,

The Honorable Thomas S. Foley
Page 3

and deny the Committee with expertise the ability to bring that expertise to bear on an important issue.

Sincerely,



JOHN D. DINGELL
CHAIRMAN

cc: Mr. Wm Holmes Brown, Parliamentarian
U.S. House of Representatives

The Honorable Jack Brooks, Chairman
Committee on the Judiciary

The Honorable Hamilton Fish, Ranking Member
Committee on the Judiciary

The Honorable Carlos Moorhead, Ranking Member
Committee on Energy and Commerce

The Honorable Ed Markey, Chairman
Subcommittee on Telecommunications and Finance

The Honorable Jack Fields, Ranking Member
Subcommittee on Telecommunications and Finance



515 North Washington Street
Alexandria, Virginia 22314-2357
Phone (703) 836-6767
Cable Address IACPOLICE

President
Sylvester Daughtry, Jr.
Chief of Police
Greensboro, NC

Immediate Past President
Steven R. Harris
Chief of Police
Redmond, WA

First Vice President
John T. Whetzel
Chief of Police
Chocoma, OK

Second Vice President
David G. Walchak
Chief of Police
Concord, NH

Third Vice President
Darnell L. Sanders
Chief of Police
Frankfort, IL

Fourth Vice President
Thomas A. Constantine
Superintendent
New York State Police
Albany, NY

Fifth Vice President
Bobby D. Moody
Chief of Police
Covington, GA

Sixth Vice President
Ronald S. Neubauer
Chief of Police
St. Peters, MO

International Vice President
Ronald Hadfield
Chief Constable, GPM
West Midlands Police
Birmingham, England

Treasurer
G. H. (Gill) Kleinkecht
Associate Commissioner
for Enforcement
U.S. Immigration and
Naturalization Service
Washington, D.C.

Division of State
and Provincial Police
General Chairman
Maurice J. Hannigan
Commissioner
California Highway Patrol
Sacramento, CA

Division of State Associations
of Chiefs of Police
General Chairman
Lamy G. Vardell
Chief of Police
Williamsburg, VA

Parliamentarian
Michael R. Santos
Police Legal Advisor
City of Overland Park
Overland, KS

Executive Director
Daniel H. Rosenblatt
Alexandria, VA

September 7, 1994

The Honorable Edward J. Markey
U.S. House of Representatives
Washington, D.C. 20515

Dear Representative Markey:

On behalf of the over 13,000 Chiefs of Police who are members of the International Association of Chiefs of Police (IACP), I am writing to advise you of the IACP's strong support for the Digital Telephony Act of 1994 (H.R. 4922) and to urge your support for the enactment of this important law enforcement legislation during this session of Congress. The legislation seeks to preserve law enforcement's ability to conduct court-authorized electronic surveillance in our effort to effectively fight crime and protect the American people by ensuring that new telecommunications technology does not prevent law enforcement from conducting such court-authorized surveillances.

Over 25 years ago, Congress enacted legislation that authorized the use of court approved electronic surveillance in the investigation of the most serious crimes that threaten our society and only when other investigative techniques will not work or are too dangerous to try. Further, Congress also required the telephone companies to provide law enforcement with the technical assistance necessary to accomplish the interception. Unfortunately, new and advanced telecommunications technology is threatening law enforcement's continued ability to prevent and solve serious crimes through the use of this proven and effective investigative technique. An informal survey conducted by the FBI identified over 183 incidents where federal, state and/or local law enforcement wiretap efforts had been frustrated by technological impediments and the number of such incidents is ever increasing. Without the enactment of H.R. 4922 to require the telephone companies to ensure that their individual networks and systems can accommodate law enforcement's electronic surveillance needs, the safety of the American public will remain unnecessarily at risk.

On October 28, 1992, during the annual IACP Business Meeting, the IACP formally adopted a resolution in support of legislation to preserve the ability of law enforcement to intercept communications pursuant to court order. On behalf of our nation's Chiefs of Police, I strongly urge your support for the Digital Telephony Act of 1994 (H.R. 4922) and its enactment during this session of Congress.

Sincerely,

Sylvester Daughtry, Jr.
Sylvester Daughtry, Jr.
President



U.S. Department of Justice

Federal Bureau of Investigation

Office of the Director

Washington, D.C. 20535

April 15, 1993

Honorable Edward J. Markey
Chairman
Subcommittee on Telecommunications
and Finance
Committee on Energy and Commerce
House of Representatives
Washington, D.C.

Dear Mr. Chairman:

As you are fully aware, the Nation's telecommunications systems and networks are often used in furtherance of serious and often violent criminal activities. Court-authorized electronic surveillance is one of the most important and effective investigative techniques used by law enforcement to combat crime and protect national security. Recent advances in telecommunications technology have made it increasingly difficult for Federal, state, and local law enforcement agencies to enforce the criminal laws using this critical investigative technique. These technologies present a two-fold challenge to law enforcement: first, the ability to access communications that are subject to court-authorized interception is being jeopardized by fundamental changes in transmission formats (the digital telephony issue), and second, the ability to understand intercepted communications on a real-time basis is soon to be defeated by low cost, readily available commercial encryption devices (the encryption issue). Like other advanced digital telecommunications technologies, the ready availability of high-powered encryption now threatens to preclude the effective use of electronic surveillance.

In an effort to work towards a balanced, comprehensive national policy concerning the use of encryption with communication devices, the President has recently issued a Presidential Decision Directive regarding the use of a Government-developed key escrow encryption microcircuit called "Clipper Chip." I believe the adoption of this policy and the use of the key escrow encryption Clipper Chip technology achieve an equitable balance between the rights and needs of the American public and business to protect their communications and the legitimate need of law enforcement to conduct court-authorized electronic surveillance.

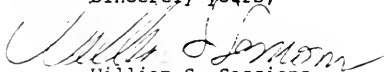


Honorable Edward J. Markey

This key escrow Clipper Chip system will provide the American public with communication encryption devices that are more secure and less expensive than other devices that are available today. At the same time, the use of the Clipper Chip will provide law enforcement with access to the plain text of encrypted conversations when court authorization has been obtained to conduct an electronic interception and encryption is encountered. The use of the key escrow encryption microcircuit by manufacturers of communication encryption devices called for by the President will prevent criminals from utilizing such devices in an effort to hide their serious criminal activity.

As Director of the FBI, I thought it important to bring to your attention the impact low cost but robust encryption will have on the ability of law enforcement to combat terrorism, violent crime and other criminal activities that many times require electronic surveillance to successfully prevent or solve. I have enclosed for your information a press statement and questions and answers addressing many of the issues surrounding this technology solution. An explanation of how this technology works is reflected in these documents. We are prepared to provide you or your staff with a detailed briefing concerning the law enforcement implications related to this matter and to address any questions you may have. Such an arrangement can be made by contacting Inspector in Charge John E. Collingwood of my Office of Public and Congressional Affairs at telephone number (202) 324-2727.

Sincerely yours,



William S. Sessions
Director

Enclosures (2)

THE WHITE HOUSE
Office of the Press Secretary

For Immediate Release

April 16, 1993

STATEMENT BY THE PRESS SECRETARY

The President today announced a new initiative that will bring the Federal Government together with industry in a voluntary program to improve the security and privacy of telephone communications while meeting the legitimate needs of law enforcement.

The initiative will involve the creation of new products to accelerate the development and use of advanced and secure telecommunications networks and wireless communications links.

For too long, there has been little or no dialogue between our private sector and the law enforcement community to resolve the tension between economic vitality and the real challenges of protecting Americans. Rather than use technology to accommodate the sometimes competing interests of economic growth, privacy and law enforcement, previous policies have pitted government against industry and the rights of privacy against law enforcement.

Sophisticated encryption technology has been used for years to protect electronic funds transfer. It is now being used to protect electronic mail and computer files. While encryption technology can help Americans protect business secrets and the unauthorized release of personal information, it also can be used by terrorists, drug dealers, and other criminals.

A state-of-the-art microcircuit called the "Clipper Chip" has been developed by government engineers. The chip represents a new approach to encryption technology. It can be used in new, relatively inexpensive encryption devices that can be attached to an ordinary telephone. It scrambles telephone communications using an encryption algorithm that is more powerful than many in commercial use today.

This new technology will help companies protect proprietary information, protect the privacy of personal phone conversations and prevent unauthorized release of data transmitted electronically. At the same time this technology preserves the ability of federal, state and local law enforcement agencies to intercept lawfully the phone conversations of criminals.

A "key-escrow" system will be established to ensure that the "Clipper Chip" is used to protect the privacy of law-abiding Americans. Each device containing the chip will have two unique

"keys," numbers that will be needed by authorized government agencies to decode messages encoded by the device. When the device is manufactured, the two keys will be deposited separately in two "key-escrow" data bases that will be established by the Attorney General. Access to these keys will be limited to government officials with legal authorization to conduct a wiretap.

The "Clipper Chip" technology provides law enforcement with no new authorities to access the content of the private conversations of Americans.

To demonstrate the effectiveness of this new technology, the Attorney General will soon purchase several thousand of the new devices. In addition, respected experts from outside the government will be offered access to the confidential details of the algorithm to assess its capabilities and publicly report their findings.

The chip is an important step in addressing the problem of encryption's dual-edge sword: encryption helps to protect the privacy of individuals and industry, but it also can shield criminals and terrorists. We need the "Clipper Chip" and other approaches that can both provide law-abiding citizens with access to the encryption they need and prevent criminals from using it to hide their illegal activities. In order to assess technology trends and explore new approaches (like the key-escrow system), the President has directed government agencies to develop a comprehensive policy on encryption that accommodates:

- the privacy of our citizens, including the need to employ voice or data encryption for business purposes;
- the ability of authorized officials to access telephone calls and data, under proper court or other legal order, when necessary to protect our citizens;
- the effective and timely use of the most modern technology to build the National Information Infrastructure needed to promote economic growth and the competitiveness of American industry in the global marketplace; and
- the need of U.S. companies to manufacture and export high technology products.

The President has directed early and frequent consultations with affected industries, the Congress and groups that advocate the privacy rights of individuals as policy options are developed.

The Administration is committed to working with the private sector to spur the development of a National Information Infrastructure which will use new telecommunications and computer technologies to give Americans unprecedented access to information. This infrastructure of high-speed networks ("information superhighways") will transmit video, images, HDTV programming, and huge data files as easily as today's telephone system transmits voice.

Since encryption technology will play an increasingly important role in that infrastructure, the Federal Government must act quickly to develop consistent, comprehensive policies regarding its use. The Administration is committed to policies that protect all American's right to privacy while also protecting them from those who break the law.

Further information is provided in an accompanying fact sheet. The provisions of the President's directive to acquire the new encryption technology are also available. ..

For additional details, call Mat Heyman, National Institute of Standards and Technology, (301) 975-2758.

QUESTIONS AND ANSWERS ABOUT THE CLINTON ADMINISTRATION'S
TELECOMMUNICATIONS INITIATIVE

- Q: Does this approach expand the authority of government agencies to listen in on phone conversations?
- A: No. "Clipper Chip" technology provides law enforcement with no new authorities to access the content of the private conversations of Americans.
- Q: Suppose a law enforcement agency is conducting a wiretap on a drug smuggling ring and intercepts a conversation encrypted using the device. What would they have to do to decipher the message?
- A: They would have to obtain legal authorization, normally a court order, to do the wiretap in the first place. They would then present documentation of this authorization to the two entities responsible for safeguarding the keys and obtain the keys for the device being used by the drug smugglers. The key is split into two parts, which are stored separately in order to ensure the security of the key escrow system.
- Q: Who will run the key-escrow data banks?
- A: The two key-escrow data banks will be run by two independent entities. At this point, the Department of Justice and the Administration have yet to determine which agencies will oversee the key-escrow data banks.
- Q: How strong is the security in the device? How can I be sure how strong the security is?
- A: This system is more secure than many other voice encryption systems readily available today. While the algorithm will remain classified to protect the security of the key escrow system, we are willing to invite an independent panel of cryptography experts to evaluate the algorithm to assure all potential users that there are no unrecognized vulnerabilities.
- Q: Whose decision was it to propose this product?
- A: The National Security Council, the Justice Department, the Commerce Department, and other key agencies were involved in this decision. This approach has been endorsed by the President, the Vice President, and appropriate Cabinet officials.

- Q: Who was consulted? The Congress? Industry?
- A: We have on-going discussions with Congress and industry on encryption issues, and expect those discussions to intensify as we carry out our review of encryption policy. We have briefed members of Congress and industry leaders on the decisions related to this initiative.
- Q: Will the government provide the hardware to manufacturers?
- A: The government designed and developed the key access encryption microcircuits, but it is not providing the microcircuits to product manufacturers. Product manufacturers can acquire the microcircuits from the chip manufacturer that produces them.
- Q: Who provides the "Clipper Chip"?
- A: Mykotronx programs it at their facility in Torrance, California, and will sell the chip to encryption device manufacturers. The programming function could be licensed to other vendors in the future.
- Q: How do I buy one of these encryption devices?
- A: We expect several manufacturers to consider incorporating the "Clipper Chip" into their devices.
- Q: If the Administration were unable to find a technological solution like the one proposed, would the Administration be willing to use legal remedies to restrict access to more powerful encryption devices?
- A: This is a fundamental policy question which will be considered during the broad policy review. The key escrow mechanism will provide Americans with an encryption product that is more secure, more convenient, and less expensive than others readily available today, but it is just one piece of what must be the comprehensive approach to encryption technology, which the Administration is developing.

The Administration is not saying, "since encryption threatens the public safety and effective law enforcement, we will prohibit it outright" (as some countries have effectively done); nor is the U.S. saying that "every American, as a matter of right, is entitled to an unbreakable commercial encryption product." There is a false "tension" created in the assessment that this issue is an "either-or" proposition. Rather, both concerns can be, and in fact are, harmoniously balanced through a reasoned, balanced approach such as is proposed with the "Clipper Chip" and similar encryption techniques.

- Q: What does this decision indicate about how the Clinton Administration's policy toward encryption will differ from that of the Bush Administration?
- A: It indicates that we understand the importance of encryption technology in telecommunications and computing and are committed to working with industry and public-interest groups to find innovative ways to protect Americans' privacy, help businesses to compete, and ensure that law enforcement agencies have the tools they need to fight crime and terrorism.
- Q: Will the devices be exportable? Will other devices that use the government hardware?
- A: Voice encryption devices are subject to export control requirements. Case-by-case review for each export is required to ensure appropriate use of these devices. The same is true for other encryption devices. One of the attractions of this technology is the protection it can give to U.S. companies operating at home and abroad. With this in mind, we expect export licenses will be granted on a case-by-case basis for U.S. companies seeking to use these devices to secure their own communications abroad. We plan to review the possibility of permitting wider exportability of these products.

FACT SHEETPUBLIC ENCRYPTION MANAGEMENT

The President has approved a directive on "Public Encryption Management." The directive provides for the following:

Advanced telecommunications and commercially available encryption are part of a wave of new computer and communications technology. Encryption products scramble information to protect the privacy of communications and data by preventing unauthorized access. Advanced telecommunications systems use digital technology to rapidly and precisely handle a high volume of communications. These advanced telecommunications systems are integral to the infrastructure needed to ensure economic competitiveness in the information age.

Despite its benefits, new communications technology can also frustrate lawful government electronic surveillance. Sophisticated encryption can have this effect in the United States. When exported abroad, it can be used to thwart foreign intelligence activities critical to our national interests. In the past, it has been possible to preserve a government capability to conduct electronic surveillance in furtherance of legitimate law enforcement and national security interests, while at the same time protecting the privacy and civil liberties of all citizens. As encryption technology improves, doing so will require new, innovative approaches.

In the area of communications encryption, the U.S. government has developed a microcircuit that not only provides privacy through encryption that is substantially more robust than the current government standard, but also permits escrowing of the keys needed to unlock the encryption. The system for the escrowing of keys will allow the government to gain access to encrypted information only with appropriate legal authorization.

To assist law enforcement and other government agencies to collect and decrypt, under legal authority, electronically transmitted information, I hereby direct the following action to be taken:

INSTALLATION OF GOVERNMENT-DEVELOPED MICROCIRCUITS

The Attorney General of the United States, or her representative, shall request manufacturers of communications hardware which incorporates encryption to install the U.S. government-developed key-escrow microcircuits in their products. The fact of law

enforcement access to the escrowed keys will not be concealed from the American public. All appropriate steps shall be taken to ensure that any existing or future versions of the key-escrow microcircuit are made widely available to U.S. communications hardware manufacturers, consistent with the need to ensure the security of the key-escrow system. In making this decision, I do not intend to prevent the private sector from developing, or the government from approving, other microcircuits or algorithms that are equally effective in assuring both privacy and a secure key-escrow system.

KEY-ESCROW

The Attorney General shall make all arrangements with appropriate entities to hold the keys for the key-escrow microcircuits installed in communications equipment. In each case, the key holder must agree to strict security procedures to prevent unauthorized release of the keys. The keys shall be released only to government agencies that have established their authority to acquire the content of those communications that have been encrypted by devices containing the microcircuits. The Attorney General shall review for legal sufficiency the procedures by which an agency establishes its authority to acquire the content of such communications.

PROCUREMENT AND USE OF ENCRYPTION DEVICES

The Secretary of Commerce, in consultation with other appropriate U.S. agencies, shall initiate a process to write standards to facilitate the procurement and use of encryption devices fitted with key-escrow microcircuits in federal communications systems that process sensitive but unclassified information. I expect this process to proceed on a schedule that will permit promulgation of a final standard within six months of this directive.

The Attorney General will procure and utilize encryption devices to the extent needed to preserve the government's ability to conduct lawful electronic surveillance and to fulfill the need for secure law enforcement communications. Further, the Attorney General shall utilize funds from the Department of Justice Asset Forfeiture Super Surplus Fund to effect this purchase.



NATIONAL DISTRICT ATTORNEYS ASSOCIATION

99 Canal Center Plaza • Suite 511 • Alexandria, Virginia 22314
 Telephone (703) 549-9222 Fax (703) 836-3195

Office of the President

September 2, 1994

Chairman Edward J. Markey
 Subcommittee on Telecommunications and Finance
 House Committee on Energy and Commerce
 United States House of Representatives
 Washington, DC 20515-6115

Dear Chairman Markey:

The National District Attorneys Association strongly supports the Digital Telephony Act of 1994 (HR4922) as introduced in the House of Representatives by Congressman Edwards. As the "peoples prosecutors" we are charged by our citizens to lead them in the fight against crime in every city, town and county of this nation. Our support for this legislation seeks nothing more than to preserve the surveillance capability that you, the United States Congress, and many state legislatures have already authorized.

The advent of new technologies has seriously threatened the viability of one of law enforcements' most valuable tools - the court ordered wire tap. The introduction of digital technology, as well as the anticipation of new orders of emerging technology, has the potential to render this surveillance technique impotent. We only use electronic surveillance measures as a means of last resort and in only the most serious cases. When we need to use a wiretap, however, we need the capability in real world time and cannot wait for technological developments to engineer a portal. Our ability to get a court order to begin such a surveillance depends of time sensitive information. Delays to develop technological access can, as a minimum, preclude the court order on the basis of stale information and may lead to the loss of life in the most serious situations.

In July 1994 the Board of Directors of the National District Attorneys Association, representing each state in this Union, unanimously passed a resolution supporting the Digital Telephony Act of 1994. We see, daily, what crime does to our citizens and fully understand the handicap that will be forced on law enforcement, and by implication on our citizens, by the failure of The Congress to enact this much needed legislation. We would urge that the Subcommittee on Telecommunications and Finance quickly, and with resolve, vote to pass the Digital Telephony Act of 1994.

Sincerely,

Robert L. Deschamps
 Robert L. Deschamps
 President



NATIONAL DISTRICT ATTORNEYS ASSOCIATION

99 Canal Center Plaza • Suite 510 • Alexandria, Virginia 22314

Telephone: (703) 549-9222

Fax: (703) 836-3195

RESOLUTION

CONCERNING THE DIGITAL TELEPHONY
AND
COMMUNICATIONS PRIVACY IMPROVEMENT ACT

WHEREAS, one of the most important and effective techniques used by state, local and federal law enforcement in the investigation of complex and life threatening criminal activities is the court-authorized interception of otherwise private communications (wiretapping); and

WHEREAS, 37 states and the District of Columbia, Puerto Rico and the Virgin Islands have enacted legislation authorizing their state and local law enforcement agencies to conduct court-authorized electronic surveillance and establishing administrative and judicial oversight procedures to ensure the protection of privacy interests; and

WHEREAS, approximately 56 percent of the court-authorized wiretaps conducted annually in the United States are by state and local law enforcement agencies; and

WHEREAS, both federal and state electronic surveillance statutes set forth a procedure for obtaining judicial authorization to conduct a wiretap and require the telecommunications industry and others to provide "all information, facilities, and technical assistance necessary to accomplish the interception," 18 U.S.C. Sec 2518(4) and 3124(a)(b); and

WHEREAS, the rapid and continual development of new telecommunications technologies and services present an ever increasing barrier to accomplishing the court-authorized electronic surveillance; and

WHEREAS, modifications to these new technologies and services are required to effectuate the intent of federal and state statutes to permit court-authorized electronic surveillance of the communications of persons engaged in serious and life threatening criminal conduct and protect the privacy of others; and

WHEREAS, the Digital Telephony and Communications Privacy Improvement Act (the "Act") requires the telecommunications industry, when authorized by law, to provide law enforcement with the capability of intercepting the entire content of communications of persons engaged in criminal activities, regardless of the technology involved; and

WHEREAS, the Act requires the Federal Bureau Of Investigation to provide fiscal support for the telecommunications industry to achieve this capability; and

WHEREAS, the Act enhances privacy protection for individuals using emerging technologies,

THEREFORE BE IT RESOLVED, THAT, the National District Attorneys Associations supports the Digital Telephony and Communications Privacy Improvement Act; and

BE IT FURTHER RESOLVED, THAT, this Association urge the Congress to enact the Digital Telephony and Communications Privacy Improvement Act.

Adopted by the Board of Directors July 24, 1994 (Newport Beach, California)



BOSTON PUBLIC LIBRARY



3 9999 05982 368 0

ISBN 0-16-046829-9



90000



9 780160 468292